UNIVERSIDAD DON BOSCO

FACULTAD DE INGENIERÍA

TRABAJO DE GRADUACIÓN PARA OPTAR AL GRADO DE INGENIERÍA EN CIENCIAS DE LA COMPUTACIÓN

"ESQUEMAS DE SEGURIDAD BASADOS EN VPN PARA UNA RED CORPORATIVA ENFOCADA AL CONTROL DE ACCESO UTILIZANDO LOS SERVICIOS DE SEGURIDAD AAA"

PRESENTADO POR

RIVAS CAMPOS, WILFREDO
RODRÍGUEZ BONILLA, JUAN CARLOS
SIERRA BLANCO, BRIAN BALMORE

2005

EL SALVADOR, CENTROAMERICA

Introducción..... 1
Propósito..... 4
Como esta organizada esta tesis..... 5
Objetivos..... 8
Objetivo general..... 8
Objetivos especificos..... 8
Alcances..... 9
Limitaciones..... 11
Delimitaciones..... 11
1. Estrategias de seguridad..... 13
1.1 Principios de seguridad..... 13
1.1.1 Principio del menor privilegio..... 13
1.1.2 Simplicidad..... 13
1.1.3 Principio del eslabón mas débil..... 14
1.1.4 Participacion Universal..... 15
1.2 Estrategias..... 15
1.2.1 La seguridad a traves de la oscuridad..... 15
1.2.2 Punto de control centralizado (choke point) 16
1.2.3 Seguridad basada en host..... 18
1.2.4 Seguridad basada en red..... 18
1.2.5 Defensa en profundidad..... 19
1.3 Comparación entre las estrategias de seguridad..... 21
2. Un vistazo a la seguridad……..... 22
2.1 ¿Qué es seguridad?……..... 23
2.1.1 ¿por qué la seguridad es tan importante para una organización ……..... 23
2.1.2 ¿Qué tan seguros son los sistemas?...……. 24
2.1.3 Riesgos que tienen las organizaciones en la seguridad...……. 24
2.1.4 Las vulnerabilidades..…….. 28
2.1.5 Desafíos informaticos de las empresas para disminuir el 40

riesgo…….....
2.2 ¿Por qué la educación en la seguridad es importante..……... 43
2.2.1 El sector corporativo……..... 44
2.2.2 El Gobierno..…… 45
2.2.3 Sistemas Operativos……. 46
2.3 Descripción de las personas involucras en la seguridad…… 47
2.3.1 Administrador del sistema……... 47
2.3.2 Atacantes……..... 48
2.3.3 Personas de negocios.……... 59
2.3.4 El periodista……..…… 60
2.3.5 El usuario informal.……... 60
2.3.6 El especialista en seguridad…….. 60
2.4 ¿Es la seguridad un esfuerzo inútil?……... 60
2.4.1 La seguridad a través de la oscuridad…….. 61
2.4.2 ¿Por qué es el Internet inseguro?……... 62
2.4.3 ¿Necesita ser el Internet seguro? ……... 75
2.4.4 ¿Puede ser el Internet seguro? ……..……... 76
2.5 Existen aspectos primordiales en la seguridad.……... 77
2.6 ¿Qué necesitamos proteger?……..……... 78
2.7 ¿De qué nos queremos proteger? ……..……... 79
2.7.1 Personas……..……... 80
2.7.2 Amenazas lógicas……..……... 83
2.7.3 Modos comunes de ataque.....……..…… 88
2.7.4 Catástrofes.....……..…… .....……..……..... 90
2.8 ¿Cómo nos podemos proteger? ……..…….. 91
3 Políticas y niveles de seguridad……..…… 95
3.1 Proposición de una forma de realizar el análisis para llevar a cabo la elaboración de las políticas……..……..... 96
3.2 Visión general de las políticas de seguridad…….…..... 97
3.3 ¿Qué son las políticas de seguridad? ……..... 98
3.4 ¿En qué consisten las políticas……..……... 99
3.5 ¿Quién implementará y administrará las políticas……... 99

3.6 Elementos de una política de seguridad informática…….... 100
3.7 Algunos parámetros para establecer políticas de seguridad……... 101
3.8 ¿Por qué las políticas de seguridad informatica generalmente no consiguen implementarse? …….……..…….…… 103
3.9 El Riesgo…….……..…….……..... 104
3.9.1 Analisis de riesgos…….……..…….…… 104
3.9.2 Evaluación de riesgo…….……..…….…… 105
3.9.3 Niveles de riesgo…….……..…….……... 107
3.9.4 Identificación de amenaza……..... 108
3.9.5 Evaluación de costos…….……..…….…… 108
3.9.6 Valor intrínseco…….……..…….…… 110
3.9.7 Costos derivados de la pérdida……..... 111
3.10 Estableciendo políticas estrategicas..... 111
3.11 Implementación…….....……..... 112
3.12 Auditoria y control…….....……..... 114
3.13 La política…….....……..... 114
3.13.1 Nivel Físico…….....……..... 114
3.13.2 Factor humano…….....……... 116
3.13.3 Personas ajenas al sistema……..... 118
3.14 Políticas de la red corporativa……..... 120
3.14.1 Politicas generales…….....……..... 121
3.14.2 Control de acceso a usuarios……..... 121
3.14.3 Política de respaldos…….....……..... 124
3.14.4 Política del uso del software……..... 125
3.14.5 Politica del Internet……..... 125
4 Seguridad del entorno de operaciones…….……..…….. 127
4.1 Seguridad física…….……..…….. 128
4.2 Protección del hardware…….……..……... 128
4.2.1 Acceso físico…….……..……... 128
4.2.2 Desastres naturales…….……..……... 132
4.2.3 Desastres del entorno…….……..……... 136
4.2.4 Proteccón de los datos…….……..…….. 141

4.2.5 Otros elementos..... 143
5 Implementación de seguridad antivirus..... 148
5.1 Conceptos basicos sobre virus informaticos..... 149
5.1.1 ¿Qué es un virus informático? 149
5.1.2 ¿Quién los hace? 151
5.2 Funcionamiento de los virus..... 152
5.3 Algunos métodos de infección..... 155
5.4 Clasificacón de los virus..... 158
5.5 Determinar si existe infección..... 159
5.6 Síntomas más comunes de virus..... 160
5.7 Como proceder ante una infección..... 161
5.8 Programas antivirus..... 162
5.8.1 Identificación..... 163
5.8.2 Técnicas de detección..... 165
5.8.3 Análisis heurístico..... 165
5.8.4 Eliminación..... 166
5.8.5 Comprobación de integridad..... 167
5.8.6 Proteger áreas sensibles..... 168
5.8.7 Aplicar cuarentena..... 170
5.8.8 Definiciones antivirus..... 170
5.9 Características que deben cumplir los antivirus..... 171
5.10 Software antivirus..... 172
5.11 Políticas de protección contra virus..... 175
5.11.1 Como los virus pueden infectar la red corporativa..... 175
5.11.2 Como el departamento de informática prevee o minimiza las infecciones de virus..... 177
5.11.3 Como responder o reportar la presencia de un virus..... 178
5.11.4 Notificar al departamento encargado de manejar problemas con virus cuando se han detectado archivos sospechosos..... 179
5.12 Estrategias de seguridad antivirus..... 180
5.12.1 Estrategias generales de seguridad antivirus..... 180
5.12.2 Responsabilidades del administrador de red..... 184

5.12.3 Responsabilidades del empleado..... 184
5.13 Spyware..... 186
5.13.1 ¿qué es un spyware? 186
5.13.2 ¿Como infectarse? 186
5.13.3 Señales de infección..... 186
5.13.4 Remocion de spyware..... 187
5.13.5 Prevención contra spyware..... 187
6 Routers..... 189
6.1 Motivos para crear seguridad con routers..... 190
6.2 Los router como parte de defensa en profundidad..... 191
6.2.1 Roles de los routers en las operaciones y seguridad de la red..... 191
6.2.2 Filtros de paquetes para TCP/IP..... 195
6.2.3 Aplicando filtros de paquetes: permitir ciertos protocolos o servicios..... 196
6.2.4 Aplicando filtros de paquetes: rechazando protocolos y servicios riesgosos..... 197
6.2.5 Servicios que se deben bloquear completamente en un router de perímetro..... 197
6.2.6 Algunos servicios a bloquear en el router para clientes externos..... 198
6.2.7 Filtrado de direcciones..... 199
6.3 Listas de control de acceso..... 200
6.4 Funciones del router..... 204
6.4.1 Interconectividad física..... 204
6.4.2 Interconectividad lógica..... 205
6.4.3 Cálculo de rutas y mantenimiento..... 206
6.4.4 Papel del router en las redes de área amplia..... 208
6.4.5 Routers interiores en una red..... 210
6.5 Routers de perímetro desde la perspectiva de las redes privadas..... 211
6.5.1 Escenarios de internetworking..... 211
6.5.2 Enrutamiento dentro de una red..... 212

6.5.3 Enrutamiento entre redes adyacentes..... 213
6.5.4 Enrutamiento entre redes no adyacentes..... 214
7 Firewalls..... 217
7.1 Porque usar un firewall..... 219
7.1.1 Protección de la red..... 221
7.1.2 Objetivo básico de un firewall..... 221
7.1.3 Tipos de peligros que puede evitar un firewall..... 221
7.2 Ventajas y desventajas de los firewalls..... 222
7.2.1 Ventajas..... 222
7.2.2 Desventajas..... 224
7.3 Tipos de firewall..... 226
7.3.1 Filtros estáticos a nivel de paquete..... 226
7.3.2 Firewall a nivel de circuito..... 227
7.3.3 Firewall a nivel de aplicación..... 228
7.3.4 Filtros dinámicos a nivel de paquetes..... 228
7.3.5 Firewall Proxy..... 229
7.3.6 Gateways de aplicación..... 229
7.3.7 Inspección de paquetes..... 230
7.4 Los requisitos básicos..... 231
7.5 Requisitos adicionales..... 232
7.6 Características relevantes en el firewall..... 233
7.7 Esquemas de redes con firewall..... 234
7.7.1 Screening router..... 234
7.7.2 Screened host..... 235
7.7.3 Screened host dual..... 235
7.7.4 Firewall con DMZ..... 236
7.8 Metodología para selección e instalación de firewalls..... 237
7.8.1 Preselección del producto..... 237
7.8.2 Análisis de costos..... 238
7.9 Clasificación de firewall..... 239
7.9.1 Firewall basado en software..... 239
7.9.2 FIrewall basado en hardware..... 239

7.9.3 Característcas de firewall comerciales..... 240
7.10 Conclusiones..... 242
8 IDS e IPS..... 244
8.1 IDS..... 245
8.1.1 Porque usar los IDS..... 245
8.1.2 Beneficios reales..... 247
8.1.3 Tipos de IDS..... 252
8.1.4 Ubicación de los NIDS..... 254
8.1.5 Aquitecturas de los NIDS..... 256
8.1.6 Tecnologías de detección en los IDS..... 257
8.1.7 Funcionamiento de los IDS..... 258
8.1.8 Respuestas para detección de uso indebido o ataques..... 261
8.1.9 Limitaciones de los IDS..... 262
8.1.10 Clasificación del modelo de monitoreo..... 264
8.1.11 Arquitectura de administración..... 268
8.1.12 Arquitectura de operación..... 272
8.2 Elección de un IDS específico..... 276
8.3 IPS..... 278
8.3.1 Los IPS como evolución de los IDS..... 278
8.3.2 La evolucion y las categorías de los IPS..... 280
8.4 Conclusiones..... 284
9 Criptografía, Encriptación y Autenticación..... 285
9.1 Introducción a la criptografía..... 286
9.2 Terminología..... 286
9.3 Encriptación y desencriptación..... 287
9.4 Autenticación, Integridad y no rechazo..... 288
9.5 Criptografía en comunicaciones de red..... 289
9.6 ¿En realidad que tan seguro es un algoritmo criptografico?..... 290
9.7 Usos de cripto-sistemas y autenticación en VPN..... 290
9.8 Algoritmos criptográficos..... 292
9.8.1 Algoritmos hash..... 292
9.8.2 Sistemas de llaves secretas..... 293

9.8.3 Sistemas dellaves públicas……..... 294
9.9 Algoritmos de encriptación……..... 295
9.10 Uso de las llaves simétricas con IPSec……..... 295
9.11 Uso de las llaves asimétricas con IPSec……..... 296
9.11.1 Funciones hash..... 298
9.12 Algoritmos asimétricos o algoritmos de llaves públicas…… 301
9.12.1 Autenticación y no rechazo……..... 302
9.13 Uso de función hash con IPSec……..... ... ……..... 303
9.13.1 MD5 codificado y SHA-1 codificado……..... 303
9.13.2 HMAC-MD5-96 y HMAC-SHA-1-96……..... 304
9.14 DSS (Digital Signatura Standard)……..... 305
9.15 Métodos utilizados para asegurar una VPN……..... ... 306
9.16 Esquemas de autenticación……..... 308
9.17 Certificados Digitales……..... ... ……..... 309
9.18 Seguridad de encriptación con L2TP/IPSec.……... 310
9.19 Seguridad del filtrado de paquetes……..... 311
9.20 Seguridad de autenticación……..... 312
9.21 Seguridad de autenticación para conexiones L2TP/IPSec.…….. 312
9.22 Seguridad de autorización……..... ... ……..... 313
10 Protocolos utilizados en las VPN……..... ... …..... 314
10.1 El túnel……..... ... ……..... 315
10.1.1 Entendiendo la tecnología de túnel……..... 315
10.1.2 Las ventajas de la tecnología de túnel……..... 316
10.1.3 Los componentes de un túnel……..... 317
10.1.4 Operaciones de túnel……..... ... ……..... 318
10.1.5 Formato del paquete de túnel……..... 320
10.1.6 Tipos de túneles……..... ... ……..... ... 321
10.1.7 Diferencia entre los dos tipos de túneles……..... .. 323
10.1.8 Protocolos para crear túneles……..... 323
10.2 PPP (Point to Point Protocol) ……..... ... ……..... 325
10.2.1 Operación del PPP……..... ... ……..... 326
10.2.2 Formato del paquete PPP……..... 327

10.2.3 Enlace de control PPP……..... 328
10.3 PPTP (Point to Point Tunneling Protocol) ……..... 330
10.3.1 El rol del PPP en las transacciones PPTP……..... 331
10.3.2 Los componentes de transacciones de PPTP……..... 332
10.3.3 Procesos de PPTP……..... ... ……..... 335
10.3.4 Seguridad PPTP……..... ... ……..... ... 339
10.3.5 PPTP con firewalls y routers……..... 341
10.3.6 Las ventajas y desventajas del PPTP……..... 341
10.4 L2F (Layer 2 Forwarding) ……..... ... ……..... 342
10.4.1 Los procesos del L2F……..... ... ……..... 344
10.4.2 El túnel L2F……..... ... ……..... 345
10.4.3 Seguridad L2F……..... ... ……..... 347
10.4.4 Ventajas y desventajas del L2F……..... 349
10.5 L2TP (Layer 2 Tunneling Protocol) ……..... 350
10.5.1 Componentes del L2TP……..... 352
10.5.2 Procesos L2TP……..... ... ……..... 353
10.5.3 Envios de datos a través de túneles L2TP……..... 355
10.5.4 Modos de túneles L2TP……..... 355
10.5.5 Control de conexión L2TP……..... 359
10.5.6 Seguridad en L2TP……..... ... ……..... 360
10.5.7 L2TP autenticado sobre IPSec……..... 360
10.5.8 Encriptación de datos L2TP……..... 360
10.5.9 Ventajas y desventajas del L2TP……..... 361
10.6 IPSec (Seguridad del protocolo Internet……..... 363
10.6.1 Visión general del IPSec..... 363
10.6.2 Modos túnel y trasporte……..... 370
10.6.3 Modo túnel y transporte en AH…..... 371
10.6.4 Túnel ESP frente a modo transporte……..... 372
10.6.5 Transformaciones IPSec……..... 374
10.6.6 Conjuntos de transformaciones……..... 375
10.6.7 Componentes del cifrado IPSec……..... 375
10.6.8 Visión general del IKE……..... 381

10.6.9 Funcionamiento del IPSec……..... 384
10.6.10 Asociaciones de seguridad (AS) de IPSec……..... 385
10.6.11 Cuadro de flujo del IKE e IPSec……..... 386
11 VPN...……..... ...……..... ...……..... 388
11.1 Vision general de las VPN...……..... 389
11.1.1 Que es una VPN...……..... 390
11.1.2 Porque usar las VPN...……..... 390
11.2 Como las VPN resuelven problemas de seguridad en Internet…….. 392
11.3 Ventajas de las VPN...……..... ...……..... 392
11.4 Componentes de una VPN...……..... ...……..... 394
11.4.1 Manejo de direcciones...……..... 395
11.4.2 Manejo de llaves...……..... ...……..... 395
11.4.3 Firewall...……..... ...……..... 395
11.4.4 Protocolos...……..... ...……..... 396
11.5 Esquemas de VPN...……..... ...……..... 396
11.5.1 VPN de acceso remoto...……..... ...……..... 396
11.5.2 VPN sitio a sitio……...……..... ...……..... 399
11.5.3 Las VPN voice/IP mejoradas...……..... ...……. 406
11.5.4 Las VPN coorporativas...……..... ...……..... 406
11.6 Tipos especiales de VPN...……..... 406
11.6.1 VPN pass-through...……..... ...……..... 406
11.6.2 VPN basadas en MPLS……... 407
11.6.3 VPN MPLS de capa 2...……..... ...……..... 409
11.6.4 VPN MPLS de capa3...……..... 411
11.7 Las soluciones VPN...……..... ...……..... 414
11.8 Clasificación de VPN basado en la arquitectura de implementación...……..... ...……..... 415
11.8.1 Las VPN dependientes o subcontratadas……... 415
11.8.2 Las VPN independientes o internas...……..... 417
11.8.3 Las VPN Híbridas...……..... ...……..... 418
11.9 VPN basado en arquitecturas de seguridad……... 419
11.9.1 Las VPN router a router...……..... 419

11.9.2 VPN firewall a firewall.....…… 421
11.9.3 Las client-intiated VPN.....…… 423
11.9.4 Las VPN dirigidas .....…… 424
11.10 Arquitecturas VPN basadas en capas.....…… 426
11.10.1 Las VPN de la capa de enlace.....…… 426
11.10.2 Las VPN de la capa de red ....…… 428
11.11 Arquitecturas de VPN basada en clases…… 429
11.11.1 VPN clase 0.....…… .....…… 430
11.11.2 VPN clase 1.....…… 430
11.11.3 VPN clase 2…… 431
11.11.4 VPN clase 3.....…… .....…… 432
11.11.5 VPN clase 4.....…… .....…… 433
11.12 Criterios de elección de una tecnología de VPN..... 434
11.12.1 VPN MPLS .....…… 435
11.12.2 IPSec …….. 436
11.13 Ejemplos VPN.....…… .....…… 436
11.13.1 Check Point Express.....…… .....…… 436
11.13.2 eTrust VPN.....…… .....…… 442
11.13.3 SnapGear SG635……... 444
11.13.4 NetScreen 500.....…… .....…… 447
11.13.5 Nokia Firewall/VPN.....…… 451
11.13.6 VPN F-Secure.....…… .....…… 454
11.13.7 FIrebox v100: VPN y Gigabit Firewall.....…… 455
12. Servicios de seguridad AAA..... 459
12. 1 Un vistazo al AAA..... 459
12.1.1 filosofia del AAA..... 460
12.1.2 Acerca de los servicios de seguridad AAA..... 460
12.1.3 Beneficios del AAA..... 463
12. 2 Un vistazo a TACACS+..... 463
12.2.1 Funciones claves de TACACS+..... 464
12. 3 Un vistazo a RADIUS..... 466
12. 4 Comparación de TACACS+ y RADIUS..... 467

12. 5 CSACS..... 471
13. Implementación del esquema de seguridad propuesto..... 473
13. 1 Planteamiento del problema..... 473
13. 2 Solución..... 474
13.2.1 Diseño propuesto..... 476
13.2.2 La VPN..... 477
13.2.3 Restringir el acceso general a la red interna..... 487
13.2.4 Protección de virus..... 494
13.2.5 Implementación de los recursos corporativos..... 495
13.2.6 Configuración de la computadora cliente..... 496
Recomendaciones..... 497
Conclusiones..... 503
Fuentes de Información..... 507
Glosario..... 512
Anexo 1..... 526
Anexo 2..... 532

INTRODUCCIÓN

En las organizaciones, la Seguridad de la Información (SI) ha comenzado a tomar un lugar determinante dentro de la gestión de la Tecnología de la Información (TI), y se ha convertido en un elemento fundamental a ser considerado en toda estrategia de negocio con miras a lograr metas importantes a corto, mediano y largo plazo.

En consecuencia, las organizaciones experimentan la necesidad de definir estrategias efectivas que garanticen una gestión segura de los procesos del negocio a fin de darle **integridad, confiabilidad y disponibilidad** a la información, y al mismo tiempo no poner barreras para adaptarse a los continuos cambios de la organización como resultado de las exigencias del mercado.

Tal necesidad ha impulsado el énfasis en el planteamiento de nuevos paradigmas en la seguridad informática basada en políticas y estrategias de seguridad. Sin embargo, existen interrogantes relacionadas con la manera de aplicar los cambios necesarios sin que estos impacten de manera significativa en las operaciones de una organización y que además perdure en el tiempo.

A pesar de algunos esfuerzos, es factible encontrar hoy en día ejecutivos de negocio y profesionales que continúan percibiendo la seguridad como un asunto meramente técnico que debe ser resuelto mediante la utilización de un componente tecnológico en particular. Asimismo, existe la creencia que no es necesario destinar parte del presupuesto del negocio a iniciativas de seguridad de la Información, sino que por el contrario esto podría estar incluido dentro del presupuesto de otros departamentos. Otros aun perciben que la Seguridad de la Información es un aspecto que se considera luego del proceso de diseño de aplicaciones críticas del negocio.

La permanencia de este tipo de percepciones, nos lleva a determinar que las organizaciones aun necesitan entender, analizar y afianzar la relación estratégica que existe entre sus objetivos de negocio y su postura de Seguridad. Este problema se debe principalmente al hecho que la mayoría de las organizaciones no

comprenden como las actividades de seguridad añaden valor al negocio o por el contrario, si no se tiene una apropiada dirección, restarían valor a las operaciones del negocio.

Uno de los factores críticos de éxito es comprender que el asegurar los activos de información de un negocio no es problema de identificar que tecnología en particular se va a escoger, sino en conocer cuáles son los objetivos e iniciativas del negocio y de qué forma la seguridad de la información va propiciar el logro de los mismos.

La Seguridad de la Información puede ser vista desde su rol estratégico en los procesos de negocio, al identificar con qué recursos (organización, procesos, tecnología), se debe contar para alcanzar la efectividad entre las actividades de resguardo o protección de los activos de información y la habilitación del acceso apropiado a los mismos. En este sentido, la Seguridad de la Información es un aspecto sumamente importante en la relación que se establece entre el negocio, sus clientes, socios, proveedores y empleados.

Como un proceso estratégico, la Seguridad de la Información pudiera estar enfocada en proteger los activos de información de una organización contra pérdidas o uso indebido, o focalizada a brindar acceso a los activos de información apoyando los objetivos de negocio. Uniendo estos dos conceptos – seguridad como “Protección” y seguridad como “Habilitador de Accesos” – se define de manera integral un nuevo enfoque de Seguridad en las organizaciones.

La Seguridad de la Información hoy día no es sólo un aspecto tecnológico, por el contrario, es una solución integrada de negocio que combina recursos organizacionales, procesos y tecnología. Si no se cuenta con reglas, lineamientos, responsabilidades y procedimientos predefinidos, y ante la ausencia de personal que es capacitado para la gestión del proceso, la inversión en tecnología solamente no es más que una pérdida de dinero. La seguridad de la Información como una solución integral es esencial para la transformación de este nuevo enfoque, en una plataforma

tangible, pragmática y operativa de seguridad, que brinde resultados cuantificables para el negocio.

Muchas organizaciones, instituciones y expertos en el campo de la seguridad tales como: CISCO Systems, SANS (SysAdmin, Audit, Network, Security), NSA/CSS (National Security Agency/Central Security Service), DoD (Department of Defence), FBI (Federal Bureau of Investigation), CERT (Computer Emergency Response Team), SNAC (System and Network Attack Center), CSI (Computer Security Instituti), CSRC (Computer Security Resource Center), WatchGuard, Aruba Network, CyberGuard, 3COM, Borderware, ISS (Internet Security Systems), CheckPoint, MCAFEE, SYMANTEC, entre otras, basan el desarrollo de tecnología y su protección en la estrategia de seguridad Defensa en Profundidad la cual permite brindar la debida confianza, integridad y disponibilidad de la información para aquellas personas que forman parte del negocio. Es importante conocer que existen otras estrategias de seguridad (que se mencionan en el capitulo 1) las cuales pueden ser utilizadas según las necesidades y recursos de las organizaciones, es decir la importancia que tenga la seguridad para cada organización.

Nota: para obtener mas información que confirma la implementación de la estrategia de seguridad “defensa en profundidad” por parte de estas compañías o instituciones, ver anexo 1.

PROPÓSITO.

El contenido que se muestra en esta tesis da a conocer de forma general algunas de las alternativas de seguridad que se tienen a disposición (Firewalls, IDS, IPS, Routers, Antivirus, VPN). Además, proporciona los conocimientos y criterios necesarios para poder crear, elegir o seleccionar entre varias políticas, tecnologías (equipos y protocolos) y/o esquemas de seguridad basados en VPN.

El proposito de la tesis es el siguiente.

- Dar a conocer los componentes que forman parte de la estrategia de seguridad "defensa en profundidad", con énfasis especial en políticas de seguridad y esquemas de seguridad basados en vpn.

- Proporcionar características generales que se deben tomar en cuenta al momento de seleccionar, adquirir e implementar una tecnología especifica.

- Enfocar la seguridad desde una perspectiva administrativa y técnica ya que se cubren aspectos relacionados con el desarrollo de políticas, identificación y análisis de las distintas amenazas tanto internas como externas, así como medidas preventivas que respaldan la seguridad informática y configuraciones de los distintos componentes que implementan esta seguridad.

COMO ESTA ORGANIZADA LA TESIS

Se han elaborado once capitulos, cada uno con la información necesaria para lograr el proposito y los objetivos de esta tesis, por ejemplo en el CAPITULO 1 se dan a conocer varias estrategias de seguridad cada una con sus ventajas, y desventajas con el fin de ampliar el conocimiento de las estrategias disponibles. El CAPITULO 2 proporciona una introducción a lo que es Seguridad y su importancia. Con los CAPITULOS 3,4 y 5 se proporcionan los conocimientos acerca de politicas, importancia y forma de aplicarlas. El objetivo de los capitulos 6,7 y 8 es brindar información de las tecnologías existentes en cuanto a dispositivos de seguridad (hardware y Software) y como estas pueden ser implementadas. En los CAPITULOS 9 y 10 se proporciona los elementos utilizados en la implementacion de una VPN. Y por ultimo el CAPITULO 11 da a conocer los esquemas de seguridad basados en VPN, integrando elementos de capitulos anteriores. Cada uno de los capitulos se ha elaborado con cada uno de los componentes de la estrategia Defensa en Profundidad

Capitulo 1: Estrategias de seguridad.

Da a conocer las diferentes estrategias de seguridad que estan disponibles y que se pueden utilizar para implemetar un esquema de segurida. Incluyendo sus caractertistica.

Capitulo 2: Vistazo a la seguridad.

Proveer un concepto de seguridad donde se describen las distintas formas de ataques, pérdidas, vulnerabilidades importancia, quienes son los atacantes de que se quiere proteger, forma de que forma se puede lograr esta protección.

Capitulo 3: Políticas y niveles de seguridad.

Proporciona los lineamientos necesarios para diseñar y crear las políticas que cada organización necesite.

Capitulo 4: Seguridad del entorno de operaciones.

Suministra diferentes políticas de forma general para proteger los dispositivos que forman parte de la red corporativa de daños físicos,

Capitulo 5: Implementación de seguridad antivirus.

Provee información general sobre el concepto de virus, funcionamiento, tipos existentes y como actúan, Así también como eliminarlos (software antivirus) y que políticas y estrategias implementar para poder contrarrestar este problema.

Capitulo 6: Routers.

Provee características generales, funciones, motivos para la seguridad, enrutamiento de los routers y cual es el aporte de este componente en la defensa en profundidad.

Capitulo 7: Firewalls.

Dar a conocer que es un firewall, tipos disponibles y la forma en que estos protegen la red, además, se tienen algunos criterios que se deben tomar en cuenta al momento de adquirir un firewall.

Capitulo 8: IDS e IPS.

Proporcionar de los conocimientos acerca del papel que juegan en la seguridad, con que objetivo se utilizan, tipos disponibles y criterios de selección.

Capitulo 9: Criptografía, encriptación y autenticación.

Muestra los distintos algoritmos y funciones criptográficas que son necesarias para el protocolo IPSec, así también, descripción de los algoritmos para encriptación y autenticación.

Capitulo 10: Protocolos utilizados en las VPN.

Describe los protocolos necesarios para la creación de una VPN, tipos de túneles y componentes de cifrado para IPSec.

Capitulo 11: VPN.

Introducir a las VPN y como estas se basan en las tecnologías de protección descritas en capítulos anteriores, se dan a conocer los diferentes esquemas disponibles y sus características, así como también, criterios de selección de una tecnología en especial.

Capitulo 12: SERVICIO DE SEGURIDAD AAA

Describe que es el modelo de seguridad AAA y además se da a conocer los protocolos mas utilizados con los que puede trabajar este modelo los cuales son: TACACS+ y RADIUS.

Capitulo 13 Implementación de una opción de seguridad aplicando Defensa en Profundidad.

Se describe el diseño de la red, los elementos que la componen y cual es el objetivo de su utilización, y las configuraciones de cada dispositivo

OBJETIVOS

GENERAL

“Describir los esquemas de seguridad basados en VPN más utilizados y las estrategias de protección contra ataques internos y de virus, implementando un prototipo de topología de red que permita el acceso a los recursos que se encuentran en una red corporativa utilizando los servicios de Autorización, Autenticación y Contabilidad”.

ESPECIFICOS

1. Descripción de los esquemas de de protección basadas en VPN y estrategias de protección interna contra ataques y virus.

2. Definir políticas de seguridad de los usuarios tanto internas como externas de la red corporativa.

3. Implementación de un prototipo de topología que permita el control de acceso a servicios corporativos utilizando los servicios de Autorización, Autenticación y Contabilidad.

4. Elaborar un documento que muestre el proceso de instalación y configuración del prototipo de red.

5. Definir una estrategia de protección contra virus para la red interna.

ALCANCES

1. Se describirán los esquemas de seguridad VPN.

2. Se establecerán políticas de seguridad internas que permitan tener un mejor control sobre los usuarios de la red corporativa.

3. Se implementará una estrategia de protección contra virus para la red corporativa.

4. Se implementará un prototipo de topología de red WAN en donde se utiliza equipo tales como: Router, PIXFirewall, CSACS/Radius, un servidor LINUX para permitir la comunicación segura entre los clientes remotos que desean acceder a los recursos y/o servicios de la red corporativa.

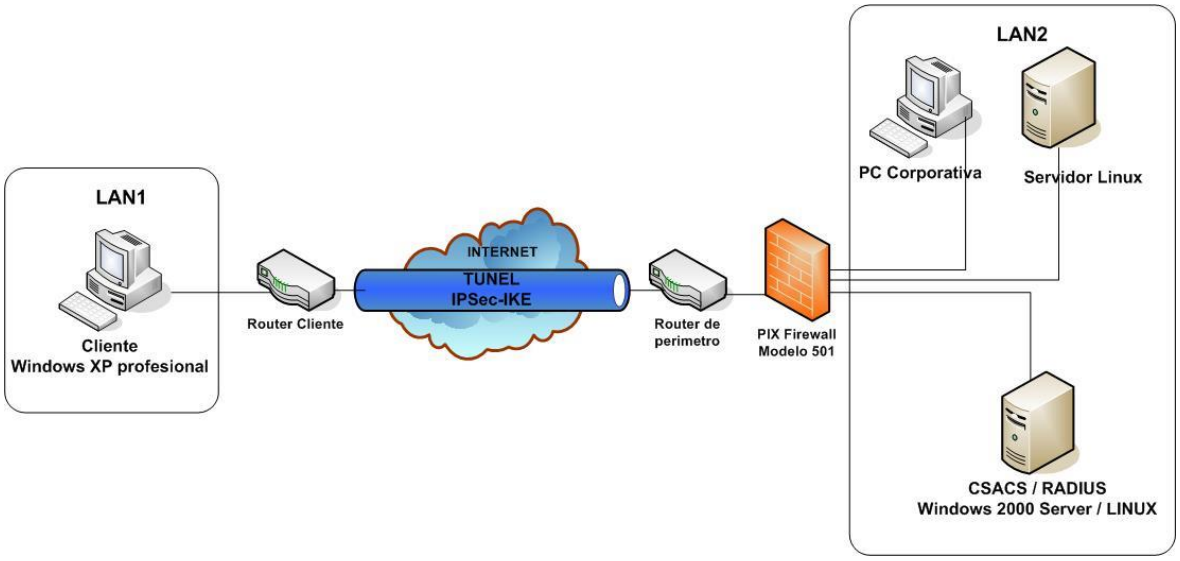


Figura 1. Diseño de topología de red propuesto para una comunicación segura.

5. Se configuraran los dispositivos de Internetworking por medio del IOS de cada uno de ellos.

6. Creación de un túnel virtual a través de la configuración de una VPN de punto a punto basada en Intranet para asegurar la integridad y confiabilidad de los datos que viajan en la red pública.

7. Configuración del conjunto de protocolos IPSec para llevar a cabo la encriptación, autenticación y criptografía de los paquetes de datos que intercambian los clientes y la red corporativa.

8. Se implementará un PIX Firewall para mantener al margen los usuarios no autorizados fuera de la red corporativa y proporcionar protección para varios tipos de ataques posibles.

9. Se hará uso de un CSACS/ Radius que se basa en el modelo de seguridad AAA el cual le indicará al PIXFirewall que usuarios pueden acceder a los recursos y nivel de autorización. Los niveles de seguridad definidos son los siguientes:

    a. Administrador.
    b. Usuario corporativo.
    c. Invitado.

10. Implementar con un servidor Linux los recursos y/o servicios que ofrece una verdadera red corporativa: WEB, FTP, Telnet, Mail, Base de Datos.

LIMITACIONES

1. La implementación del prototipo de topología de red a utilizar se verá limitado por el equipo disponible y puede no ser el óptimo.

DELIMITACIONES

1. Instalar un prototipo de red que estará compuesto de dos extremos, en un extremo se configurará una Lan representada por una PC con un router como enlace al otro punto y el otro extremo estará estructurado con un router, un PIX Firewall, un servidor CSACS y el servidor Linux que brindara los recursos corporativos.

2. Configurar los routers para establecer comunicación y un Pix Firewall para proteger los recursos de la red corporativa de los posibles accesos no autorizados desde Internet. Las configuraciones solo están aplicadas a equipos pertenecientes a Cisco.

3. Configurar el Servidor de Control de Acceso Seguro de Cisco (CSACS) y RADIUS para administrar el acceso de los usuarios hacia los recursos de la red corporativa.

4. Con el prototipo de topología de red propuesta no se pretende ofrecer una solución cien por ciento efectiva contra ataques a una red corporativa

5. Los sistemas operativos a utilizar en el prototipo de red propuesto serán:

    a. Cliente: Microsoft Windows XP Professional.
    b. CSACS/Radius: Microsoft Windows 2000 Server/Linux.
    c. Servidor de los recursos: Linux.

6. El protocolo a utilizar para la encriptación, autenticación y criptografía de los paquetes que viajan en el túnel virtual será el protocolo IKE de IPSec.

7. Los dispositivos de internetworking a utilizar solamente se les hará la configuración necesaria para el debido funcionamiento en el prototipo de red propuesto.

8. Para la configuración de los router Cisco se utilizará el protocolo RIP, IGRP y EIGRP.

9. El PIX Firewall a utilizar en esta topología de red será el modelo 501.

10. El modelo de topología de red es basado en protocolos IP

11. El manual de usuario será entregado solamente en formato de video en CD.

CAPITULO 1. ESTRATEGIAS DE SEGURIDAD

1.1. Principios de seguridad

Antes de describir las estrategias de seguridad se deben de tomar en cuenta algunos principios fundamentales al plantear cualquier estrategia de seguridad.

1.1.1. Principio de menor privilegio.

Este es quizás el principio más fundamental de la seguridad, y no solamente de la informática. Básicamente, el principio de menor privilegio afirma que cualquier objeto (usuario, administrador, programa, sistema, etc.) debe tener tan solo los privilegios de uso necesarios para desarrollar su tarea y ninguno más. Esto quiere decir que cualquier usuario tan solo debe poder acceder a los recursos que necesite, para realizar las tareas que tenga encomendadas y sólo durante el tiempo necesario.

Al diseñar cualquier política de seguridad es necesario estudiar las funciones de cada usuario, programa, etc., definir los recursos a los que necesita acceder para llevarlas a cabo, identificar las acciones que necesita realizar con estos recursos, y establecer las medidas necesarias para que tan solo pueda llevar a cabo estas acciones.

1.1.2. Simplicidad.

La simplicidad es un principio de seguridad por dos razones. En primer lugar, mantener las cosas lo más simples posibles, las hace más fáciles de comprender. Si no se entiende algo, difícilmente puede saberse si es seguro. En segundo lugar, la complejidad permite esconder múltiples fallos. Los programas más largos y complejos son propensos a contener múltiples fallos y puntos débiles.

Características:

- Los sistemas muy complejos tienden a tener fallas y huecos de seguridad.
- La idea es mantener los sistemas tan simples como sea posible, eliminando funcionalidad innecesaria.
- Sistemas simples que tienen mucho tiempo, han sido tan depurados que prácticamente no tienen huecos de seguridad.

1.1.3. Principio del eslabón más débil.

En todo sistema de seguridad, al igual que en la vida real la cadena siempre se rompe por el eslabón más débil, en un sistema de seguridad el atacante siempre acaba encontrando y aprovechando los puntos débiles o vulnerabilidades.

Cuando diseñemos una política de seguridad o establezcamos los mecanismos necesarios para ponerla en práctica, debemos contemplar todas las vulnerabilidades y amenazas. No basta con establecer mecanismos muy fuertes y complejos en algún punto en concreto, sino que hay que proteger todos los posibles puntos de ataque.

Por ejemplo, se establece una política de asignación de passwords muy segura en la que estos se asignan automáticamente, son aleatorios y se cambian cada semana. Si en nuestro sistema utilizamos la red ethernet para conectar nuestras máquinas y no protegemos la conexión, no nos servirá de nada la política de passwords establecida.

Por defecto, en la red ethernet los passwords circulan de manera no cifrada. Si cualquiera puede acceder a la red y "escuchar" todos los paquetes que circulan por la misma, es seguro que pueda conocer los passwords. En este sistema el punto débil es la red. Por mucho que se refuerce la seguridad en otros puntos, el sistema sigue siendo altamente vulnerable.

La mayor desventaja es que aunque se realice un análisis profundo y se tengan todas las políticas bien definidas, siempre habrá un aspecto que no se tome en cuenta.

1.1.4. Participación universal.

Para que cualquier sistema de seguridad funcione es necesaria la participación universal, o al menos no la oposición activa, de los usuarios del sistema. Prácticamente cualquier mecanismo de seguridad que se establezca puede ser vulnerable si existe la participación voluntaria de algún usuario autorizado para romperlo.

La participación voluntaria de todos los usuarios en la seguridad de un sistema es el mecanismo más fuerte conocido para hacerlo seguro. Si todos los usuarios prestan su apoyo y colaboran en establecer las medidas de seguridad y en ponerlas en práctica el sistema siempre tenderá a mejorar.

La gran desventaja de esta estrategia de seguridad es que NUNCA se debe confiar completamente en el usuario.

1.2. Estrategias.

A continuación se describen varias estrategias de seguridad, proporcionando algunas características ventajas y desventajas de cada una de ellas con el objetivo de ampliar el conocimiento de las estrategias disponibles.

- La seguridad a través de la oscuridad
- Punto de control centralizado (choke point).
- Seguridad basada en host
- Seguridad basada en red
- Defensa en profundidad (a varios niveles)

1.2.1. La seguridad a través de la oscuridad.

Un sistema no es más seguro porque se escondan sus posibles defectos o vulnerabilidades, sino porque se conozcan y corrijan estableciendo las medidas de

seguridad adecuadas. El hecho de mantener posibles errores o vulnerabilidades en secreto no evita que existan, y de hecho evitan que se corrijan.

No es una buena medida basar la seguridad en el hecho de que un posible atacante no conozca las vulnerabilidades del sistema. Los atacantes siempre disponen de los medios necesarios para descubrir las debilidades más insospechadas del sistema.

No se consigue proteger un sistema evitando el acceso de los usuarios a la información relacionada con la seguridad. Por ejemplo, evitando el acceso a determinados manuales donde se especifican las ordenes que pueden utilizarse para entrar en el sistema. Educar a los usuarios o diseñadores sobre el funcionamiento del sistema y las medidas de seguridad incluidas, suele ser mejor método para protegerlo.

No obstante tampoco se trata de hacer público un nuevo fallo del sistema o un método para romperlo.

1.2.2. Punto de control centralizado (choke point).

Se trata de establecer un único punto de acceso a nuestro sistema, de modo que cualquier atacante que intente acceder al mismo tenga que pasar por él. No se trata de utilizar un sólo mecanismo de seguridad, sino de "alinearlos" todos de modo que el usuario tenga que pasar por ellos para acceder al sistema.

Este único canal de entrada simplifica nuestro sistema de defensa, puesto que nos permite concentrarnos en un único punto. Además nos permite monitorear todos los accesos o acciones sospechosas.

El Firewall ofrece seguridad mediante el uso de Choke Point, monitoreos y Políticas de seguridad, determinando que servicios de la red pueden ser accesados y quienes pueden utilizar estos recursos, manteniendo al margen a los usuarios no-autorizados.

Las políticas son el pilar de este sistema, informan a los usuarios de sus responsabilidades, normas de acceso remoto o local, políticas de acceso a los recursos de la red, reglas de encriptación, normas de protección de virus y entrenamiento.

El administrador del Firewall puede definir el choke-point o (embudo), para mantener al margen a los usuarios no-autorizados (hackers, crakers, vándalos y espías). Si aparece alguna actividad sospechosa genera una alarma ante la posibilidad de que ocurra un ataque.

Características y ventajas

- Protección de la Red. Mantiene alejados a los piratas informáticos (crakers) de su red al mismo tiempo que permite el acceso a todo el personal de la oficina.
- Control de acceso a los recursos de la red. Al encargarse de filtrar, en un primer nivel, antes que lleguen los paquetes al resto de las computadoras de la red, el Firewall es idóneo para implementar en él los controles de acceso.
- Control de uso de Internet. Permite bloquear el material no adecuado, determinar qué sitios puede visitar el usuario de la red interna y llevar un registro.
- Concentra la seguridad. Él facilita la labor a los responsables de seguridad, dado que su máxima preocupación es encarar los ataques externos y vigilar manteniendo un monitoreo.
- Control y estadísticas. Permite controlar el uso de Internet en el ámbito interno, conocer los intentos de conexiones desde el exterior y detectar actividades sospechosas.
- Choke-Point. Permite al administrador de la red definir un embudo manteniendo al margen los usuarios no-autorizados y prohibiendo potencialmente la entrada o salida.
- Genera Alarmas de Seguridad. El administrador del Firewall puede responder una alarma y examina regularmente los registros de base.

- Audita y registra Internet. Permite al administrador de red justificar el gasto que implica la conexión a Internet, localizando con precisión los cuellos de botella potenciales del ancho de banda.
- Se hace pasar todo el tráfico de la red por un solo punto y se enfocan los esfuerzos de seguridad en ese punto.
- Puede disminuir el rendimiento.

1.2.3. Seguridad basada en host

Los mecanismos de seguridad están en los hosts, puede ser diferente en cada host, lo cual hace difícil su instalación y mantenimiento. Si un host es atacado con éxito, peligra la seguridad de la red (muchos usuarios tienen el mismo *login* y *password* en todos los hosts a los que tienen acceso).

- Los mecanismos de seguridad están en los hosts.
- Los mecanismos de seguridad pueden ser diferentes en cada host, lo cual hace difícil su instalación y mantenimiento.
- Amedida que el número de host aumenta su administración y mantenimiento es más difícil.
- Si se encuentra una vulnerabilidad en el sistema es necesario corregir la vulnerabilidad en todos los hosts afectados.

1.2.4. Seguridad basada en red

Los ataques a nivel de red siguen siendo bastante frecuentes. Aunque las pilas TCP/IP de los distintos sistemas operativos son cada vez más robustas, todavía son frecuentes los ataques de denegación de servicio en servidores debidos al empleo de generadores de datagramas IP erróneos o complicados de procesar.

Es también frecuente el empleo de herramientas automatizadas de escaneo y comprobación de vulnerabilidades en redes, así como la utilización de programas

específicos que explotan una determinada vulnerabilidad de un servidor o servicio concreto para atacarlo.

Filtrado de paquetes

Es importante que estos filtros determinen las condiciones de acceso a los servicios permitidos. Aunque el filtrado es difícil de implementar correctamente, a las organizaciones deberian implementar sus propios filtros en función a sus necesidades y a su topología de red concreta.

El mejor modo de realizar esto es restringir la entrada en la interfaz externa (filtro de entrada), no permitiendo que un paquete entre a la red si tiene la dirección origen de la red interna. De la misma forma, se deberán filtrar los paquetes salientes que tengan una dirección origen distinta a la correspondiente a la red interna (con esto último se evitarán ataque de IP-spoofing originados desde la red).

Características:

- La seguridad se basa en controlar los accesos a los hosts desde la red.
- El método más común es la implementación de *firewalls*.
- Es un sistema de defensa que restringe conexiones TCP/IP, el lenguaje que entiende un firewall es: Any, Pass, Block y drop, que mediante reglas o políticas son ejecutadas.

1.2.5. Seguridad en redes basada en la estrategia "defensa en profundidad"

Esta tesis no es estrictamente una guía que proporcione configuraciones de equipo sin el debido entendimiento del porque se esta configurando de esta forma; más bien se ha **Enfocado a la seguridad en redes basada en la estrategia "defensa en profundidad"** orientado a un propósito fundamental el cual es lograr una mejor educación en el área de la seguridad informática. Proporcionando puntos claves que necesitan una especial atención y que deben tratarse con prioridad dentro de los

procesos de la organización. Además proporcionará referencias muy importantes sobre la seguridad y el manejo que las organizaciones tendrán para proveer una protección consistente contra el robo y la no disponibilidad de los datos.
Defensa en profundidad es una proposición de múltiples capas de seguridad que son mejores que un solo mecanismo de protección, las capas pueden ser tecnológicas, procedimientos o políticas. Defensa en profundidad incrementa la seguridad de un una corporación ya sea pequeña mediana o grande. Actualmente es recomendada por las instituciones antes mencionadas y por nosotros en esta tesis. Para consultar acerca del concepto visitar.
http://www.nsa.gov/about/about00019.cfm#6.

Defensa en profundidad es una estrategia de vanguardia que esta siendo utilizada por compañías que se dedican a la investigación y desarrollo de tecnologías nuevas de seguridad en redes. Además por todos los beneficios que proporciona, la tendencia hoy en día esta orientada a la utilización de dicha estrategia. Para mayor referencia consultar ANEXO 1.

Defensa en profundidad es una estrategia de seguridad muy versátil ya que toma los elementos de otras estrategias y los integra de manera que su funcionamiento sea más efectivo. Como ejemplo. La estrategia “basada en host” proporciona solamente un nivel de seguridad el cual es relativamente fácil de violar igualmente se puede hablar de la estrategia de seguridad de red. Esta estrategia se basa en un nivel de seguridad el cual resulta fácil de violar.

1.3. Comparación entre las estrategias de seguridad.

A continuación en la siguiente tabla se muestran algunas ventajas importantes de cada estrategia de seguridad.

ESTRATEGIAS	CONFIABILIDAD	NIVEL DE ADMINISTRACION[1]	FACTOR HUMANO[2]	COSTOS
La seguridad a través de la oscuridad	baja	bajo	bajo	variado
Punto de control centralizado (choke point).	alta	medio	bajo	bajo
Seguridad basada en host	media	alto	alto	medios
Seguridad basada en red	media	bajo	bajo	medios
Defensa en profundidad	alta	alto	bajo	alto

Tabla 1.1 Comparacion de las distintas estrategias de seguridad.

[1] Se refiere al nivel de complejidad que se tiene desde el punto de vista de administración y gestion de cada estrategia.
[2] El nivel de importancia del papel que juegan las personas para que la estrategia fucione de forma adecuada.

CAPITULO 2. VISTAZO A LA SEGURIDAD.

La seguridad es un concepto muy importante que las corporaciones deben tener en cuenta para proteger su información de una forma que no sea modificada, Interceptada, fabricada o interrumpida. En este capitulo se brinda el concepto de seguridad y describe información acerca de:

Puntos clave:

- Cómo las organizaciones pueden ser atacadas y quienes producen esos ataques.

- Los desafíos informáticos que las empresas tienen para disminuir el riesgo.

- Porque la duración en informática es importante.

- Mecanismos de seguridad que posteriormente combinados ayudaran a formar la estrategia de seguridad “defensa en profundidad”.

2. ¿QUE ES SEGURIDAD?

En el mundo de negocios globalizados de hoy en día la seguridad es una necesidad básica que no se puede pasar por alto. Ya sea para asegurar un equipo contra desastres o contra ataques remotos. Además la seguridad siempre tiene que estar en la mente de un administrador de una red; porque muchos de los ataques pueden ser evitados ya que son cometidos por la ignorancia o el descuido.

La seguridad informática se ha ido incrementando considerablemente, dadas las cambiantes condiciones y las nuevas plataformas de computación disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes que permiten explorar más allá de las fronteras de la organización.

La seguridad es una característica de cualquier sistema informático o no informático, la cual nos indica que ese sistema esta libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible.

Ésta característica, particularmente para el caso de sistemas operativos o redes de computadores, es muy difícil de conseguir, “según la mayoría de expertos, imposible”. Se suaviza la definición de seguridad y se pasa a discutir sobre la fiabilidad la cual es: la probabilidad de que un sistema se comporte estable o cumpla sus funciones de la mejor manera posible durante un determinado tiempo.

2.1.1 ¿Por qué la seguridad es tan importante para una organización?

Con las amenazas cada vez más frecuentes y complejas, una violación a la seguridad podría ser devastadora para una organización al afectar sus operaciones, la reputación corporativa y la confianza de los clientes y accionistas. Por su parte, los gobiernos han comenzado a crear reglamentaciones diseñadas para garantizar que las empresas implementen suficientes controles de seguridad. Lo importante es que cada empresa tome conciencia de su responsabilidad frente a los accionistas,

empleados y progresivamente con el gobierno para garantizar que no se comprometan los sistemas que tienen información operativa.

2.1.2. ¿Qué tan seguro son los sistemas?

Los equipos con acceso al Internet no están 100% seguros a menos que se cierren todos los servicios de la red; medida que no es factible para las empresas. Por lo tanto cuando se habla de seguridad al mismo tiempo se esta hablando de adoptar una serie de medidas, políticas y procedimientos para que sea más difícil comprometer el acceso al sistema o a la red.

2.1.3. Riesgos que tienen las organizaciones en la seguridad.

Las vulnerabilidades pretenden describir las debilidades y los métodos más comunes que se utilizan para poner en riesgo a los equipos y a la información de las organizaciones. Los ataques pueden estar motivados por diversos objetivos, incluyendo fraude, extorsión, robo de información confidencial, venganza, acceso no autorizado a un sistema, anulación de un servicio o simplemente el desafío de penetrar un sistema.

a. Cuantificación de las vulnerabilidades

Un análisis de las vulnerabilidades de seguridad publicadas y los ataques registrados durante el año 2003 revela cuales son los sistemas operativos con más vulnerabilidades y que reciben más ataques.

La empresa británica mi2g ha recogido las diferentes alertas de seguridad publicadas y ha analizado el impacto de las mismas en los diversos sistemas operativos.

Los incidentes en función de los diversos sistemas operativos se descubre que las diferentes versiones de Windows están afectadas por un 44% de las vulnerabilidades, seguido de Linux con un 19%, las diferentes variantes de BSD con 9% y Solaris solo con un 7%. En comparación, únicamente un 0,5% de las

vulnerabilidades anunciadas durante los diez primeros meses del presente año afectan a SCO Unix y un 1,9% de las mismas afectaban a Mac OS y a Tru64 de Compaq.
Se ha analizado un total de 57.977 ataques contra sistemas informáticos realizados durante el mismo periodo de tiempo. El sistema operativo más atacado han sido las diferentes versiones de Windows, con 31.431 ataques que equivale a un 54% del total, seguido nuevamente por Linux con 17.218 ataques que es el 30%, BSD con el 6% y Solaris únicamente con el 5%.

Los otros sistemas operativos tienen un volumen de incidentes registrado casi despreciable: sólo 31 ataques registrados contra sistemas ejecutando Mac OS que es equivalente a un 0,05%. Los otros sistemas operativos situados en la parte inferior de ésta escala son SCO Unix con 165 ataques que equivalen al 0,2% y Tru64 de Compaq con 10 ataques con solo el 0,02%.

Otros sistemas operativos se ven beneficiados de lo que se conoce como "security by obscurity" y que podría traducirse como "seguridad a través de la oscuridad". Entre estos sistemas tenemos a IRIX de SGI que si bien está afectado por un 6% de las vulnerabilidades sólo ha registrados dos ataques. Otro caso es AIX de IBM, afectado por un 4% de las vulnerabilidades y que únicamente ha sido atacado en 199 incidentes.

Si se desea mayor información acerca de los incidentes y Estadísticas visitar http://www.cert.org/stats/cert_stats.html.

La repercusión económica de estos ataques para las corporaciones en los últimos años han sido enormes. A continuación se detalla en las siguientes gráficas.

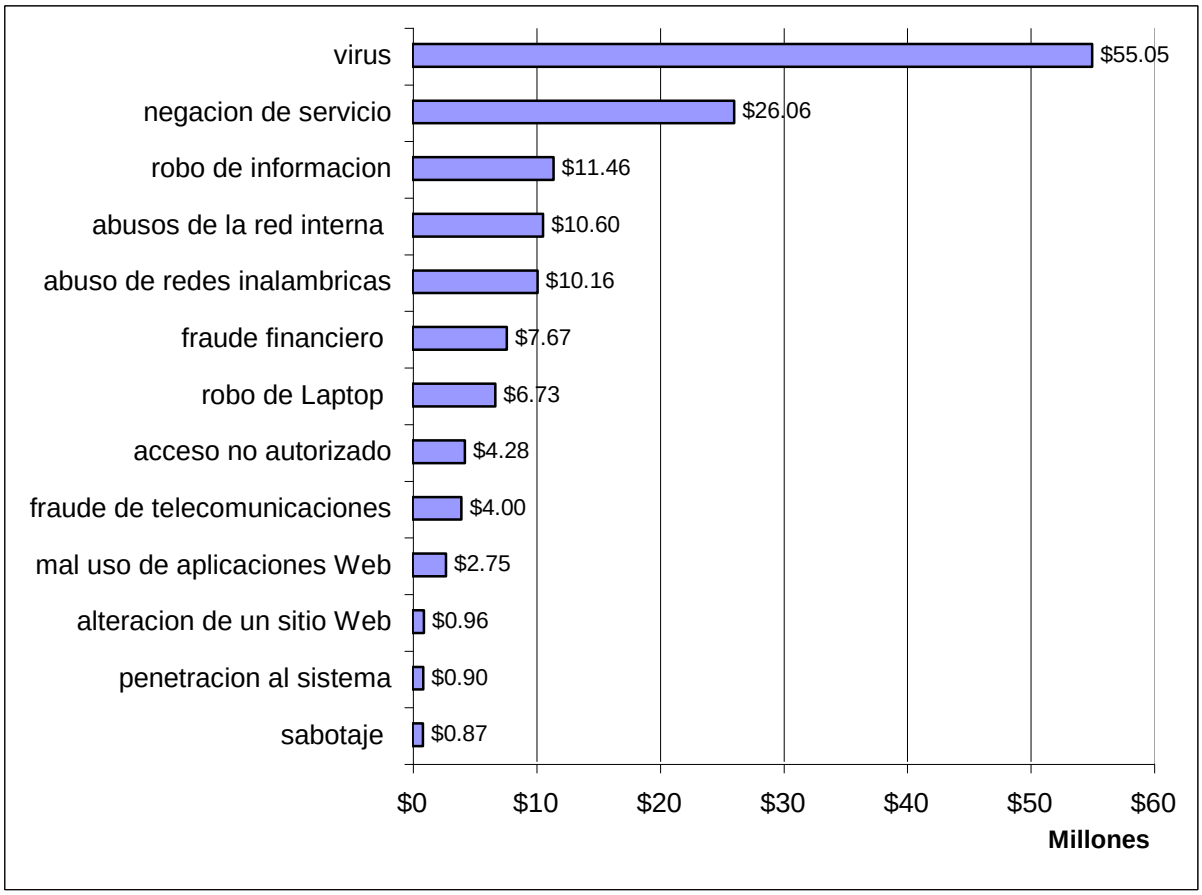


Gráfico 2.1 Pérdida económicas de las empresa en el 2004 fuente: CSI/FBI Computer Crime and Security Survey

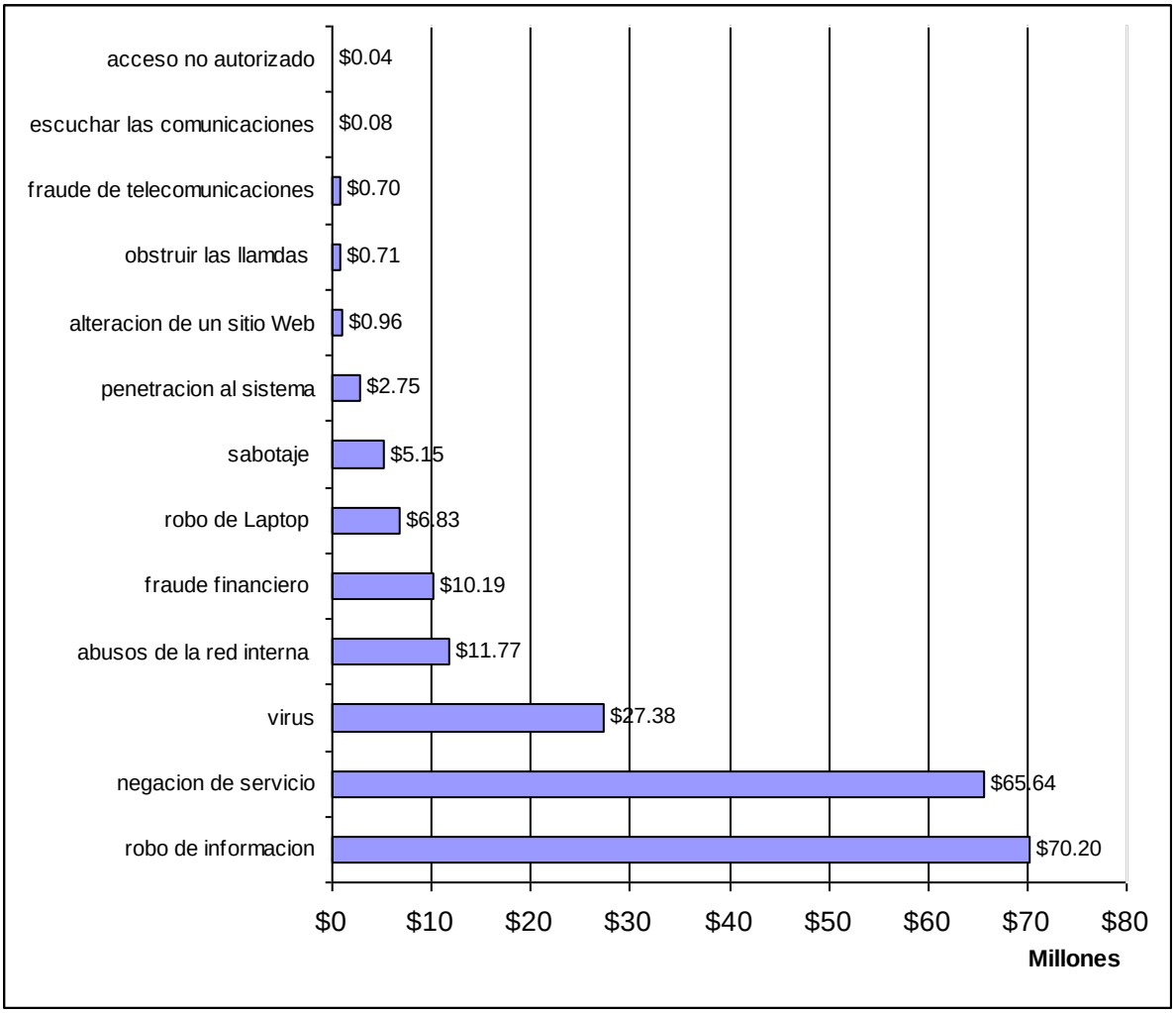


Gráfico 2.2 Pérdida económicas de las empresa en el 2003 fuente: CSI/FBI Computer Crime and Security Survey

Los ataques ocasionan miles de millones de pérdidas todos los años, por lo que las organizaciones no pueden ignorar más el problema. El Virus “Love Bug” en el 2000 ocasionó pérdidas por 8,75 millones de dólares e hizo que las empresas finalmente reconocieran que los virus son un gran problema y comenzaran a implementar ampliamente soluciones antivirus.

Tres aspectos importantes han incentivado el aumento de los incidentes de seguridad: las vulnerabilidades, los procesos de trabajo intensivo que se requieren para combatir las vulnerabilidades y la complejidad de los ataques.

2.1.4. Las vulnerabilidades.

El término vulnerabilidad hace referencia a defectos pequeños que contienen nuestros sistemas y que pueden producir consecuencias no deseadas en la seguridad de la organización.

Las vulnerabilidades se pueden clasificar según dos criterios: numero de paquetes a emplear e información necesaria para llevar a cabo el ataque.

- Número de paquetes a emplear en el ataque puede ser:
  - Atómico: se requiere un único paquete para llevarla a cabo.
  - Compuesto: son necesarios múltiples paquetes.
- Información necesaria para llevar a cabo el ataque puede ser:
  - Contexto: se requiere únicamente información de la cabecera del protocolo. Ejemplo de ataques son: Ping of death, Land attack, WinNuke, Port scan, SYN Flood, TCP hijacking.
  - Contenido: es necesario también el campo de datos o payload. Ejemplo de ataques son: ataque DNS, Proxied RPC, ataque IIS, ataques SMTP, String matches, Sniffing.

2.1.4.1 Vulnerabilidades que afectan a todos los sistemas.

Las vulnerabilidades que a continuación se van a describir son: la base de la mayoría de los ataques exitosos, que suelen aprovecharse de las brechas más conocidas con las herramientas de ataque más efectivas y fáciles de conseguir. La mayoría de los atacantes, simplemente se aprovecha de quienes no actualizan su software.

Nota: Según el FBI (Federal Bureau of Investigation) y SANS (SysAdmin, Audit, Network, Security), las organizaciones deberían mantener sus sistemas actualizados con las nuevas versiones en el mercado para prevenir la mayoría de los ataques cometidos por intrusos.

a. Instalaciones por defecto de sistemas y aplicaciones.

La mayoría del software, incluyendo sistemas operativos y aplicaciones, vienen con scripts o programas de instalación cuya meta es dejar los sistemas operativos lo más rápido posible, con la mayor parte de funciones disponibles o habilitadas y con la ayuda de muy poco trabajo por parte del administrador. Para lograr esta meta, los scripts instalan más componentes de los que realmente necesitan, debido a que la filosofía de los fabricantes es que resulta mejor habilitar funciones que no son utilizadas a que el usuario instale funciones adicionales a medida que las vaya requiriendo.

Las instalaciones por defecto suelen incluir programas de demostración que no son realmente necesarios. Una de las peores vulnerabilidades en los servidores web son los script de ejemplo, ya que los atacantes usan estos scripts para comprometer el sistema u obtener información acerca de éste.

Esta situación genera la mayoría de las vulnerabilidades de seguridad. Porque, muchos usuarios no son conscientes de lo que están realmente instalado en sus propios sistemas, dejando peligrosos programas instalados en sus PC, en cuanto a los sistemas operativos, las instalaciones por defecto casi siempre incluyen extraños servicios con sus correspondientes puertos abiertos y, de esta forma, los atacantes se introducen en ellos, por medio de dichos puertos. Por esta razón, cuantos menos puertos se hallen abiertos, mayor seguridad tendrá el sistema.

b. Cuentas sin contraseña o contraseñas débiles.

La mayoría de los sistemas se encuentran configurados para usar contraseñas secretas como primera y única línea de defensa. Sin embargo, los nombres de usuario son relativamente fáciles de conseguir, por lo que si un atacante puede determinar el nombre de una cuenta y su contraseña correspondiente, puede entrar a la red de la organización.

Ante esta situación, las contraseñas fáciles de adivinar y las contraseñas por defecto constituyen dos grandes problemas, aunque el mayor problema viene de las cuentas sin contraseñas.

Muchos sistemas contienen cuentas que vienen incluidas o cuentas por defecto. Estas cuentas generalmente tienen la misma contraseña para todas las instalaciones del software, por lo que los atacantes buscan esas cuentas por ser conocidas en su comunidad. Por esta razón, cualquier cuenta preexistente o por defecto debe ser identificada y eliminada del sistema.

c. Copias de seguridad (backups) incompletos o inexistentes.

Siempre que ocurre un incidente, la recuperación de los datos requiere copias de seguridad actualizadas y métodos probados para restaurar la información.
Algunas organizaciones hacen backups diarios, pero nunca verifican que éstos se encuentren realmente funcionando.

Tales errores son normalmente descubiertos después de que un atacante ha entrado en los sistemas y ha destruido o arruinado la información. Por otro lado, un segundo problema es la insuficiente protección física de dicha copia de seguridad, ya que suelen contener la misma información sensible que reside en los servidores y debe, por tanto, ser protegido de la misma forma.

Por seguridad, los backups deben realizarse diariamente, aunque en la mayoría de las organizaciones se realiza uno completo una vez a la semana y copias increméntales todos los días. Además, el soporte del backup debe verificarse al menos una vez al mes, mediante la restauración de un servidor de prueba que permita ver si la información se está salvando correctamente.

d. Gran número de puertos abiertos.

Tanto los usuarios legítimos como los atacantes se conectan a los sistemas por medio de puertos. Así, cuantos más puertos se encuentren abiertos más formas hay para que alguien se conecte. Por esta razón, es importante mantener abiertos sólo

los puertos imprescindibles para que el sistema funcione correctamente y el resto deben ser cerrados.

e. Insuficiente filtrado de los paquetes con direcciones de inicio y destino inadecuadas.

La falsificación de direcciones IP es un método comúnmente utilizado por los atacantes para cubrir sus huellas cuando atacan a una víctima. Así por ejemplo, el popular ataque “smurf” hace uso de una característica de los routers para enviar una secuencia de paquetes a miles de máquinas. Cada paquete contiene una dirección IP de origen que es suplantada por la de una víctima. Las maquinas a las que estos paquetes falsificados son enviados inundan a la máquina víctima deteniendo sus servicios.

f. Registro de eventos (logging) incompleto o inexistente.

Mientras que se permite fluir el tráfico entre la red de un sistema e Internet, existen probabilidades de que un atacante se introduzca en ella silenciosamente. Una vez atacado, sin registros (logs) hay muy pocas probabilidades de que se descubra qué hicieron realmente los atacantes.

Sin esa información la organización afectada debe elegir entre recargar completamente el sistema operativo desde el soporte original y luego esperar que los backups se encuentren en buenas condiciones, o bien asumir el riesgo que representa seguir utilizando un sistema que un atacante controla.

Los registros proporcionan los detalles de lo que está ocurriendo, qué sistemas se encuentran bajo ataque y qué sistemas han sido comprometidos.

g. Programas CGI vulnerables.

La mayoría de los servidores web, incluyendo IIS de Microsoft y Apache, permiten el uso de programas CGI (Commom Gateway Interface) para proporcionar interactividad a las páginas web, habilitando funciones tales como: recolección de información y verificación. De hecho, la mayoría de los servidores web vienen con

programas CGI de ejemplo preinstalados. Sin embargo, demasiados programadores de CGIs pasan por alto el hecho de que sus programas proporcionan un vínculo directo entre cualquier usuario, en cualquier parte de Internet, y el sistema operativo en la máquina que se encuentra ejecutando el servidor Web.
Los programas CGI vulnerables resultan especialmente atractivos para los intrusos, ya que son relativamente fáciles de localizar y de operar con los mismos privilegios y poder que tiene el software del servidor Web. De esta forma, los atacantes abusan de los programas CGI para modificar páginas Web, robar información de tarjetas de crédito e instalar puertas traseras para tener acceso a los sistemas comprometidos. Por esta razón, los programas de ejemplo deben ser siempre eliminados de los sistemas de producción.

2.1.4.2. Las vulnerabilidades de Linux/Unix.

A continuación se describen las diez vulnerabilidades más recientes y críticas que pueden hacer estragos en los sistemas Unix

a. Software BIND.

BIND es el software estándar de facto para actuar como servidor de nombres de dominio, un servicio esencial para el correcto funcionamiento de la red, ya que se encarga de la conversión de los nombres de dominio a sus correspondientes direcciones IP.

Determinadas versiones de BIND son vulnerables a ataques que pueden ser utilizados por un atacante remoto para comprometer los sistemas vulnerables. Adicionalmente, una mala configuración de BIND puede revelar información sensible sobre la configuración de la red.

Es importante verificar que los sistemas que ejecuten BIND utilicen la versión más reciente, incluso si esto supone abandonar la versión distribuida por el fabricante del sistema operativo e instalar la versión del ISC a partir de su código fuente.

b. Servidor Web.

Prácticamente todos los sistemas Unix incluyen de forma nativa el servidor Apache. Una configuración inadecuada del mismo así como la utilización de versiones antiguas pueden provocar problemas de seguridad, con diversos niveles de efectos sobre el nivel de seguridad.

c. Autenticación.

Es habitual encontrar equipos Unix con deficiencias en sus mecanismos de autenticación. Esto incluye la existencia de cuentas sin contraseña (o con contraseñas ampliamente conocidas o fácilmente deducibles). Por otra parte es frecuente que diversos programas (o el propio sistema operativo) cree nuevas cuentas de usuario con un débil mecanismo de autenticación.

d. Sistemas de control de versiones.

El sistema de control de versiones más utilizado en entornos Unix es CVS. Si la configuración del servidor CVS permite conexiones anónimas a determinadas versiones que son susceptibles a ataques que producen desbordamiento de búfer pueden ser utilizados para ejecutar código arbitrario en el servidor.

e. Servicio de transporte de correo.

Los equipos Unix que actúan como servidores de correo pueden ser vulnerables, caso de utilizar una versión antigua, a todo tipo de ataques. Fruto de estos ataques se puede conseguir el control completo del sistema vulnerable, la utilización del servidor de correo como estación de distribución de distribución de correo basura o robo de información sensible.

f. Protocolo SNMP.

El protocolo SNMP se utiliza de una forma masiva para la gestión y configuración remota de todo tipo de dispositivos conectados a la red: impresoras, routers, puntos de acceso, ordenadores.

Dependiendo de la versión de SNMP utilizada, los mecanismos de autenticación son muy débiles. Adicionalmente diversas implementaciones del protocolo son vulnerables a todo tipo de ataques, que van desde la denegación de servicio, a la modificación no autorizada de la configuración de los dispositivos o incluso de la consola donde se centraliza la gestión de la red.

g. Biblioteca OpenSSL.

En los últimos meses se han detectado diversas vulnerabilidades en la biblioteca OpenSSL que afectan a un gran número de productos que hacen uso de la misma: Apache, CUPS, Curl, OpenLDAP, s-tunnel, Sendmail y muchos otros.

Es importante verificar que se está utilizando la versión más reciente de OpenSSL y todos los productos que utilizan OpenSSL para el cifrado de la información.

h. Mala configuración de los servicios de red.

Los servicios NFS y NIS son los métodos más frecuentemente utilizados para la compartición de recursos e información entre los equipos Unix de una red. Una mala configuración de los mismos puede ser utilizada para la realización de diversos tipos de ataques, que van desde la ejecución de código en los sistemas vulnerables a la realización de ataques de denegación de servicio.

i. Bases de datos.

Las bases de datos son un elemento fundamental para la mayoría de las empresas. Prácticamente cualquier aplicación empresarial está construida alrededor de una base de datos donde se almacena información altamente sensible y vital para el funcionamiento del negocio.

Los problemas de configuración, una mala política de control de acceso, errores en las aplicaciones, errores de diseño o la complejidad intrínseca de muchos entornos puede ser el origen de problemas de seguridad que afecten a la integridad, fiabilidad y/o disponibilidad de los datos.

j. Núcleo del sistema operativo.

El núcleo del sistema operativo realiza las funciones básicas como la interacción con el hardware, la gestión de la memoria, la comunicación entre procesos y la asignación de tareas. La existencia de vulnerabilidades en el núcleo puede provocar problemas de seguridad que afecten a todos los componentes del sistema. Es muy importante la correcta configuración del núcleo, para evitar o reducir el alcance de las posibles vulnerabilidades.

2.1.4.3. Las vulnerabilidades de los sistemas Windows.

A continuación se describen las diez vulnerabilidades más recientes y criticas que pueden hacer estragos en los sistemas Windows:

a. Existencia de servidores web y sus servicios asociados.

Cuando se instala un servidor web en un equipo Windows, en su configuración por defecto, se activan algunos servicios y/o configuraciones que son vulnerables a diversos tipos de ataques, que van desde la denegación de servicio hasta el compromiso total del sistema. Es necesario tener actualizado el servidor web y fortalecido con buenas configuraciones.

Es importante indicar que algunas versiones de Windows instalan, en su configuración por defecto, el servidor web IIS.

b. Servicio Workstation.

Existe una vulnerabilidad de desbordamiento de búfer en el servicio Workstation de Windows 2000 (SP2, SP3 y SP4) y Windows XP (hasta SP1) que puede ser utilizada por un usuario remoto para forzar la ejecución de código en los sistemas vulnerables. Éste código se ejecutará en el contexto de seguridad SYSTEM, lo que permite un acceso completo en el sistema comprometido.

c. Servicios de acceso remoto de Windows.

Todas las versiones de Windows incluyen mecanismos para permitir el acceso remoto tanto a las unidades de disco y al registro así como para la ejecución remota de código. Estos servicios han demostrado ser bastante frágiles y la existencia de numerosas vulnerabilidades. Además han sido uno de los mecanismos preferidos por los gusanos y virus para propagarse.

Es muy importante verificar que se han aplicado las diversas actualizaciones publicadas para impedir las acciones de los mismos.

d. Microsoft SQL Server.

El gestor de base de datos de Microsoft ha sido, tradicionalmente, un producto con un nivel de seguridad muy bajo.

Existen un gran número de vulnerabilidades de seguridad, muchas de ellas críticas, que pueden ser utilizadas para acceder y/o modificar la información almacenada en las bases de datos.

Pero además, la configuración por defecto de Microsoft SQL Server facilita que sea utilizado como plataforma para la realización de ataques contra otros sistemas. Podemos recordar los gusanos SQLSnake y Slammer que tuvieron un efecto perceptible en toda la red Internet.

e. Autenticación de Windows.

Es habitual encontrar equipos Windows con deficiencias en sus mecanismos de autenticación. Esto incluye la existencia de cuentas sin contraseña (o con contraseñas ampliamente conocidas o fácilmente deducibles). Por otra parte es frecuente que diversos programas (o el propio sistema operativo) cree nuevas cuentas de usuario con un débil mecanismo de autenticación.

Por otra parte, a pesar de que Windows transmite las contraseñas cifradas por la red, dependiendo del algoritmo utilizado es relativamente simple aplicar ataques de

fuerza bruta para descifrarlos en un plazo de tiempo muy corto. Es por tanto muy importante verificar que se este utilizado el algoritmo de autenticación NTLMv2.

f. Navegadores web.

Los diversos navegadores habitualmente utilizados para acceder a la web pueden ser un punto débil de las medidas de seguridad si no se han aplicado las últimas actualizaciones.

Internet Explorer es, sin duda, el producto para el que se han publicado más actualizaciones y que cuenta con algunos de los problemas de seguridad más críticos. No obstante debe recordarse que otros navegadores como Opera, Mozilla, Firefox y Netscape también tienen sus vulnerabilidades de seguridad.

g. Aplicaciones de compartición de archivos.

Las aplicaciones P2P se han popularizado en los últimos años como un sistema para la compartición de información entre los usuarios de Internet, hasta el punto de convertirse en uno de los métodos preferidos para obtener todo tipo de archivos. De hecho, muchos usuarios seguramente no entenderían la red actual sin la existencia de las aplicaciones P2P.

No obstante, algunas aplicaciones populares de compartición de archivos tienen serios problemas de seguridad que pueden ser utilizados por un atacante para obtener el control del ordenador del usuario.

Otro riesgos habituales, no estrictamente de seguridad pero si relacionado ya que atentan contra nuestra privacidad, son los diversos programas espías incluidos en algunas de las aplicaciones más populares de compartición de archivos. Otro problema habitual es la compartición inadvertida de archivos que contienen información sensible.

En los últimos meses se ha popularizado la utilización de las redes P2P como un nuevo mecanismo para la distribución de virus y gusanos.

h. Subsistema LSAS.

El subsistema LSAS (Local Security Authority Subsystem) de Windows 2000, Windows Server 2003 y Windows XP es vulnerable a diversos ataques de desbordamiento de búfer que pueden permitir a un atacante remoto obtener el control completo del sistema vulnerable. Esta vulnerabilidad ha sido explotada por gusanos como el Sasser.

i. Programa de correo.

Diversas versiones de Windows incluyen de forma estándar el programa de correo Outlook Express. Se trata de un producto que, si no se encuentra convenientemente actualizado, puede fácilmente comprometer la seguridad del sistema.

Los principales problemas de seguridad asociados a Outlook Express son la introducción de virus (sin que sea necesario ejecutar ningún programa) y el robo de información sensible.

Las versiones actuales de Outlook Express, configuradas de una forma adecuada, protegen al usuario ante estos problemas de seguridad.

j. Sistemas de mensajería instantánea.

La mensajería instantánea ha pasado de ser un sistema de comunicación utilizado básicamente para contactar con amigos y familiares a ser una herramienta de comunicación habitualmente utilizada en las empresas, especialmente entre aquellas que disponen de diversos centros de trabajo.

Los diversos programas de mensajería instantánea pueden ser víctimas de ataques explotables de forma remota y que pueden ser utilizados para obtener el control de los sistemas vulnerables.

La solución del sector informático a estas vulnerabilidades es suministrar reparaciones en forma de revisiones informáticas que el personal de una organización debe aplicar para “tapar” el “agujero”. El proceso de probar estas

revisiones y aplicarlos en su entorno es una labor intensiva. Generalmente es muy difícil tratar las vulnerabilidades de más alto nivel y este problema se ha intensificado por el crecimiento asombroso de nuevas vulnerabilidades. Las vulnerabilidades registradas en el año 2003 aumentaron en un 300% en comparación con las registradas en el 2000.

La complejidad de los ataques a la seguridad también ha aumentado significativamente en los últimos años. Los primeros virus causaban problemas de productividad individual, aunque no tenían el impacto de las amenazas combinadas como Código Rojo o Nimda. Como mencionamos anteriormente, las amenazas combinadas utilizan una combinación de vectores de ataque —cinco en el caso de Nimda— para propagarse más rápidamente y causar más daños que un simple virus. Por ejemplo, Código Rojo infectó 350.000 computadoras en sólo 14 horas. En enero de 2003, el gusano Slammer atacó Internet y tuvo un promedio de infección más alto que Código Rojo, llegando a infectar 75.000 equipos en menos de 10 minutos después de su ataque.

El gusano de correo masivo que se propagó más rápidamente hasta la fecha fue MyDoom en enero de 2004. En pleno ataque, más de 100.000 clases de gusanos fueron interceptados por hora. MyDoom dependía de las personas para activarse y poderse propagar. Se disfrazaba inteligentemente como un archivo anexo de texto inofensivo para que los usuarios desprevenidos abrieran este archivo anexo y activaran el gusano.

La rápida propagación de estas amenazas hace muy difícil responder con la suficiente rapidez para evitar los daños. Se espera que las amenazas sigan creciendo en magnitud, velocidad y complejidad, lo que dificulta aún más su prevención y eliminación. Estos factores contribuyen a la necesidad de contar con un plan proactivo para solucionar los problemas de seguridad de la información en las en las corporaciones.

2.1.5. Desafíos informáticos de las empresas para disminuir el riesgo.

Convencidas o no, actualmente, las organizaciones deben enfrentarse con más urgencia al desafío tecnológico para tener seguros sus activos y no sólo motivadas por la competencia y el mejoramiento de la relación con sus clientes y proveedores, sino también por un tema de reducción de costos operacionales, que, fundamentalmente, está empujando a las grandes compañías a ingresar a competir de una manera diferente. Por otra parte, con un significativo menor grado de avance, tanto por un tema de costos como de actitud, este reto es aún mayor para las organizaciones pequeñas.

2.1.5.1 Subir el nivel de gestión.

Aparte de los desafíos relacionados con la capacidad de las empresas de orientarse tecnológicamente en ciertas áreas informáticas, un reto importante es: subir el nivel de gestión de las organizaciones, ya que uno de los problemas a los cuales se ven enfrentados hoy día a nivel de proveedores es que muchos de quienes manejan los negocios no conocen las tecnologías y por tanto, no son capaces de decidir en torno a ellas, ni menos justificar una inversión en esta área.

El problema es que a las organizaciones suponen que la falta de tecnología todavía no les duele lo suficiente como para decidir hacer algo y erróneamente piensan que pueden seguir subsistiendo sin enfrentar este cambio tecnológico.

2.1.5.2. De la mano del cambio.

Es necesario que las organizaciones tengan en cuenta ciertos aspectos tales como:

a. Concientización del personal.

En lo referente a los secretos del éxito en materia de seguridad informática, Ken Jaworski mencionó que “Un programa efectivo de conciencia de seguridad logra cambiar el comportamiento de los empleados para que acepten su responsabilidad

de proteger la información; por este motivo, los programas deben ser dinámicos y con metas a corto plazo para que el personal vea resultados inmediatos".

Se puede crear un programa de concientización de seguridad con base en algunos aspectos tales como spyware, spam, encripción, ingeniería social, código malicioso, acceso remoto, administración del riesgo, entre otros, dependiendo de los necesidades de la organización.

Finalmente, los empleados proactivos que se involucran en las medidas de seguridad, deben de ser reconocidos para crear conciencia en el resto de los empleados.

b. Incorporación de tecnología.

La tecnología ha traído como consecuencia la caída de barreras, especialmente económicas y sociales, por ejemplo, la encriptación. Sin embargo, hay que reconocer que la utilización de la tecnología es imprescindible en la creación del valor, ya que permite ahorrar, primordialmente, el recurso tiempo, clave para la ventaja competitiva de la organización. Debido a esto se puede identificar esta época que corre con nombre y apellido como: Cambio Tecnológico.

A pesar de que es evidente la repercusión que ha tenido en el mundo actual la tecnología, ha encontrado gran resistencia, provocando la muerte de muy buenas empresas. Es innegable que la tecnología, para muchos, representa una amenaza a su seguridad, lo que provoca incomodidad y miedo, que se traduce como "angustia tecnológica".

Pero, pese a todo eso, son muchas las voces que han puesto de relieve que actualmente tiene poco sentido plantear la problemática de las nuevas tecnologías en el mundo del trabajo en términos de rechazo o aceptación ya que es un hecho demostrado que para la subsistencia de las empresas en el mundo competitivo es un factor básico la aplicación de estas tecnologías. Esto significa que, en estos tiempos, hay que poder triunfar con la tecnología y no a pesar de ella.

c. Tareas pendientes.

Existen tres aspectos en los que las empresas han tomado mucha conciencia y que están guiando sus esfuerzos en términos de orientación de sus inversiones en tecnologías de información. Estos se refieren:

- Se espera que no sea necesario que los empleados, clientes y socios tengan acceso oportuno y preciso a la información.
- La capacidad de establecer nuevos y provechosos tipos de relación y canales con sus clientes y proveedores.
- La búsqueda de la eficiencia y de la eficacia.
- La relación con la definición del negocio mismo, sus fortalezas, ventajas y debilidades.
- Las compañías deben ofrecer servicios fáciles de utilizar y totalmente seguros porque guardan información confidencial como direcciones y números de las tarjetas de crédito personales.
- Se espera que los sistemas estén disponibles las 24 horas, los 7 días de la semana porque los clientes quieren tener acceso a los productos y servicios cuando sea conveniente para ellos, no para la compañía.

Estos desafíos exigen bastante de las organizaciones de TI. A medida que crecen las expectativas, también aumentan las exigencias en cuanto a los sistemas y la tecnología. En este sentido, las empresas se están adecuando a los nuevos desafíos, aplicando los nuevos conceptos tecnológicos para alcanzar estos objetivos.
En definitiva, actualmente, la tecnología está disponible y existe capacidad para generar servicios e instalar infraestructura. Lo importante, es analizar en qué medida la sociedad está realmente haciendo uso de estos nuevos elementos, para poder tomar decisiones de cambio ya que actualmente muchas organizaciones adoptan conductas de mucha cautela esperando un escenario de mayor tranquilidad para abordar con fuerza muchos proyectos que hoy están detenidos.

2.2. ¿POR QUÉ LA EDUCACIÓN EN LA SEGURIDAD ES IMPORTANTE?

Tradicionalmente, las personas que se ocupan de la seguridad han procurado disimular la información de la seguridad al usuario final o ha personas no autorizadas que desean ganar acceso a los datos. Por esta razón, los especialistas de la seguridad ocupan posiciones de prestigio en el mundo de la computación. En alguna época estos eran vistos como altos sacerdotes o como personas inalcanzables en sus conocimientos. Porque los usuarios debían ser suministrados con información sobre una base del necesitar - saber. Sin embargo, esto se fue disminuyendo porque ahora los usuarios han alcanzado la base del necesitar - saber estados.

Así pues, se plantea la pregunta otra vez: ¿Quién necesita ser educado sobre seguridad? La respuesta es: Todos nosotros. Aunque depende de su estado de vida. Si usted es una persona comerciante o una persona de negocios, la respuesta es directa: Para conducir comercio en la red, usted debe estar seguro de algún nivel razonable en la seguridad de los datos. Esta razón también es compartida por los consumidores. Entre el consumidor y el comerciante se ve involucrada una persona en la seguridad de datos la cual viene siendo: el vendedor del software que provee las herramientas para facilitar ese comercio.
La intimidad es una preocupación. El Internet representa la primera prueba real que una sociedad puede establecer. Cada usuario debería ser consciente que la comunicación poco encriptada a través del Internet es completamente insegura. Aunque el Internet es un recurso maravilloso para la investigación o la recreación, no es su amiga por lo menos, si sé tiene algo para esconder.

Hay otras razones más concretas de promover la educación en seguridad informática y una de estas razones es que el Internet está llegando a ser más popular cada día. Debido a que más firmas de negocios introducen nuevas e innovadoras maneras de utilizar la red. Es probable que en un plazo de cinco años, el Internet se convierta en una parte importante y funcional de nuestras vidas.

2.2.1 El sector corporativo.

El sector corporativo dejó a un lado escenarios dramáticos como el espionaje corporativo. Estos temas son excitantes para los propósitos de debate, pero su incidencia real es rara. En lugar de eso, nos gustaría concentrarnos en un problema muy real: El costo.

Las bases de datos corporativas son diseñadas usando software propietario. Los honorarios de las licencias para estos paquetes grandes pueden ascender a decenas de miles de dólares. Los costos fijos de estas bases de datos incluyen la programación, el mantenimiento, y honorarios de mejoras. Abreviadamente, el desarrollo y el uso sostenido de una base de datos corporativa son costosos y de labor intensiva.

Cuando una empresa mantiene la base de datos fuera del Internet, la seguridad es una preocupación mínima. Para ser justo, un administrador debe conocer por lo menos los fundamentos en seguridad, para prevenir crackers ambiciosos que desean ganar acceso no autorizado a la red. No obstante, el número de autores potenciales es limitado y el acceso se restringe generalmente.

Ahora, tome la misma base de datos y la conecta al Internet. Repentinamente, el cuadro cambia de una forma drástica. Primero, el número de autores potenciales es ilimitado y desconocido. Un ataque podía originarse de dondequiera, aquí o en ultramar. Además, el acceso no esta limitado para uno o dos protocolos.
La operación más simple de conectar esa base de datos con el Internet abre muchas puertas de entrada. Por ejemplo, la arquitectura del acceso de la base de datos puede requerir el uso de uno o más lenguajes para llevar los datos de la base de datos a una página HTML.

Ejemplo de un escenario:
En un escenario se observaron algunos procesos. A partir del momento en que el usuario dio un click sobre el botón de submit:

- Los términos de las variables de la búsqueda sometidos por el usuario fueron extraídos y analizados por una escritura de Perl.
- La escritura de Perl alimentó las variables de un programa intermedio diseñado para interconectar con un paquete propietario de la base de datos.
- El paquete propietario de la base de datos volvió el resultado, pasándola de nuevo a una escritura de Perl que ajustó los datos a un formato HTML

Una persona que este a cargo de la seguridad puede ver que estos procesos podrían originar agujeros potenciales, dejando con una gran ventaja ha los Hacker's y a los cracker's para violar la seguridad. Exactamente por esta razón, el desarrollo de técnicas de seguridad en bases de datos es ahora un tema caliente en muchos círculos informativos.

El personal administrativo ve estos costos de seguridad como innecesarios debido a que en gran parte no entienden la naturaleza de la alternativa. La realidad es muy alarmante porque: uno o más cracker`s pueden en minutos o en horas destruir varios años de trabajo.

Las empresas para sostener su negocio en el Internet de una manera confiable deben alcanzar algún nivel aceptable de seguridad. Las compañías, ven la educación como una manera económica de lograr una seguridad mínima. Si las compañías gastan ahora en educación pueden ahorrar muchas veces el triple de esa cantidad mas tarde.

2.2.2 El gobierno.

Lo tradicional y el sentido común ambos recomiendan que los organismos gubernamentales conocen algo mas, algo especial sobre seguridad informática. Desafortunadamente, esto no es verdad, con la excepción notable de la agencia de la seguridad nacional de los Estados Unidos.

2.2.3 Sistemas operativos.

Hay rivalidad en el Internet entre los usuarios de diferentes sistemas operativos, aclaramos una cosa: No importa qué sistema operativo usted usa. A menos que sea un sistema operativo seguro, es decir, uno donde el propósito principal de su plan es: seguridad en la red, aunque siempre habrán huecos de seguridad aparentemente en otra parte.

Los estudios verdaderos han mostrado hasta hoy, menos huecos en Mac y en los sistemas operativos basados en tecnología UNIX, por lo menos en el contexto del Internet. Sin embargo, esos estudios son probablemente prematuros e inseguros.

a. Unix.

Unix es: un sistema abierto. Como tal, su código fuente está disponible para que sea examinado por todo el público. De hecho, muchos programas de UNIX vienen solamente en forma de código fuente. Otros incluyen distribuciones binarias, pero todavía incluyen el código fuente. Un ejemplo ilustrativo sería el paquete del Gopher de la universidad de Minnesota. Debido a esto, mucho se conoce sobre el sistema operativo de UNIX y sus defectos de seguridad. Porque los hackers pueden establecer el código fuente de Unix en sus hogares y así poder estudiar sus debilidades de una manera mejor.

b. Los sistemas cerrados o propietarios.

El código fuente de los sistemas operativos propietario o cerrado no es disponible. Los fabricantes de tal software furiosamente protegen su código fuente, para ser un secreto comercial.

Estos sistemas operativos propietarios se encuentran operando en la red, sus defectos de seguridad llegarán a ser fácilmente probados, en gran parte por la comunidad de cracker´s, obteniendo resultados interesantes.

Ya no vivimos en un mundo gobernado exclusivamente por un solo sistema operativo. Cundo el Internet crece en alcance y en tamaño, todos los sistemas operativos conocidos por el género humano se convierten en partes integrales de la red. Por consiguiente, la rivalidad de los sistemas operativos debe ser reemplazada por un acercamiento más sensato. La seguridad de la red depende ahora considerablemente de tener un buen conocimiento general sobre seguridad. Otro punto de vista es que: los hacker y crackers depende su éxito en gran parte del conocimiento de todas las plataformas. Así pues se pide a las personas que dejen temporalmente a un lado los prejuicios en términos del Internet, porque la seguridad de cada uno de nosotros depende.

2.3. DESCRIPCIÓN DE LAS PERSONAS INVOLUCRADAS EN LA SEGURIDAD.

Cada persona involucrada en cualquier modelo de seguridad va a necesitar diferentes técnicas para poder tener su red segura. Así como también un cracker necesitará técnicas diferentes para poder violar la seguridad. Por lo tanto cada persona encontrara de una manera distinta lograr sus objetivos. A continuación se describen las siguientes categorías:

- Un administrador de sistemas.
- Los atacantes.
- Una persona de negocios.
- Un periodista.
- Un usuario casual.
- Especialista de seguridad.

Seguidamente se detalla de una forma breve cada una de las categorías:

2.3.1. Administrador del sistema.

Un administrador de sistema es cualquier persona encargada de manejar una red o cualquier porción de una red. A veces, las personas no pueden comprender que ellos

son administradores de sistemas. Ya que en compañías pequeñas, existen personas que programan tareas, monitorean el funcionamiento de los sistemas que están corriendo, agregan nuevas cuentas de usuarios y administran los sistemas. Estas personas son consideradas como: Técnico general, de uso múltiple porque: realizan tareas informáticas a cualquier hora del día.

2.3.2. Atacantes.

Una línea de acción prudente y sabia es familiarizarse con personas que son potenciales en elaborar amenazas a los negocios de las corporaciones o a las entidades gubernamentales.

Varios nombres se conocen para los responsables que atacan las redes. Los mas comunes son: hackers, crackers, phreaks, o atacantes.

Los atacantes varían desde personas que son programadores elites hasta personas que bajan y corren Script. Las personas que bajan Script a menudo son referidas como Script Kiddies. Nunca se tiene que subestimar a los atacantes ya que la mayoría de ellos son gente altamente inteligente que conocen las vulnerabilidades de una computadora o de una red. Así como muchos profesionales en el área de las redes informáticas.

Nota: Un error grave es pensar que un Script Kiddies no es un experimentado o conocedor como un buen hacker. Las herramientas de Scripted pueden romper casi cualquier sistema con la misma facilidad que un buen Hacker. La mayoría de los ataque son llevados a cabo por Script kiddies.

Los atacantes pueden elegir formas creativas para comprometer las computadoras o las redes. Por esta razón se puede considerar fuertemente el uso de una arquitectura seguridad como es: defensa en profundidad, para contrarrestar los intentos de ataques. Ademas buscan como encontrar una brecha en la seguridad de las redes si

se implementa defensa en profundidad y sobrevive a los ataques iniciales, los atacantes sé darán por vencidos y comenzarán a buscar a su próxima víctima.

a. Motivación para los ataques

Algunas personas podrían sorprenderse al saber que no todos los hackers son malos y tampoco atacan sitios solo para causar daño. Muchos hackers piensan que debido a sus esfuerzos para quebrantar la seguridad, están haciendo que la industria se haga más fuerte, después de todo, su razón, los fabricantes están forzados a proveer seguridad más efectiva y sofisticada. Muchas veces, un atacante tiene por objetivo los sistemas operativos, aplicaciones de los vendedores, o equipo de red de los fabricantes para que estos puedan corregir sus fallas de seguridad resultando en una seguridad más fuerte para todos.

Por supuesto muchos hackers atacan los sistemas por diversión, fama, derecho de jactancia, ganancia, venganza o solo por ser destructivos.

Cualquiera que sea el motivo del hacker, la aproximación para defender una red es la misma. Construir capas de defensa para asegurar que si un atacante pasa la primera capa, la siguiente capa detiene el ataque.

b. Anatomía de un ataque de computadora

Para conocer que seguridad es requerida para detener un ataque, se debe entender como los atacantes lanzan el ataque. Este entendimiento también ayuda a reconocer cuando las redes o host dentro de una red ha estado bajo ataque.

El primer aspecto a conocer es que hay tres tipos “básicos” de ataques, como se muestran a continuación:

- **Gusano:** se propaga a si mismo a través de la red y comienza su actividad maliciosa.
- **Virus:** requiere que un usuario realice una acción como lo es abrir el archivo adjunto de un correo electrónico antes de comenzar su comportamiento malicioso. Algunas veces, si un virus se propaga el mismo afuera del host

infectado, este comenzara a propagarse de manera similar al gusano. Los virus que exhiben este comportamiento a veces son referidos como virms (gusano nacido de un virus – virus borne gusano) un nombre derivado de la fusión de las palabras virus y gusano juntos.

- **Ataque directo:** esto es cuando un hacker decide que quiere atacar un dispositivo o red específico. Este no es un ataque aleatorio. Un cierto dispositivo es la mira de un ataque, y el hacker manualmente trata de atacar sus vulnerabilidades. Este tipo de ataque generalmente hecho por una razón específica, por ejemplo, ganancia financiera, venganza o derecho de jactancia.

Cualquier ataque en contra de un servidor o host de una red tiene cinco partes básicas, como se muestra en la siguiente figura:

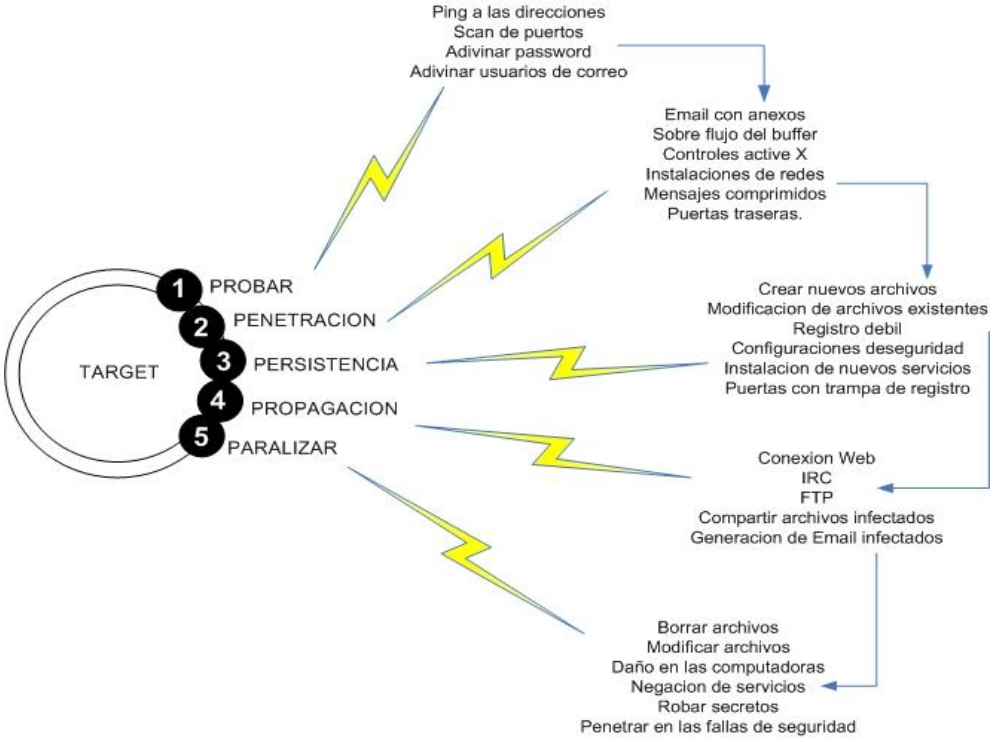


Figura 2.1 Modelo de ataque virus/gusano

La lista que sigue a continuación detalla información acerca de las cinco diferentes etapas del modelo de ataque directo de virus/worm ilustrado en la figura anterior. Esta es una lista general. Todos los ataques caen dentro de este paradigma de ataque. Por ejemplo, un virus por email puede o no puede hacer una prueba, pero su punto de inserción es aun hecho en la fase de penetración o persistencia:

1. **Probar:** los hackers deben aprender ciertas cosas básicas acerca de la red o cliente antes de saber que ataques correr. Esta es llamada la fase de prueba. Normalmente, los hackers quieren saber que tipo esta permitido dentro de la red, que servidores están accesibles desde el exterior, el sistema operativo de los servidores expuestos y las aplicaciones que están corriendo en los servidores expuestos.
2. **Penetrar:** después de que los atacantes han descubierto la información desde la fase de prueba, estos pueden chequear una de muchas bases de datos en el Internet para averiguar como atacar los servidores expuestos. Las debilidades en estos sistemas son también llamadas *vulnerabilidades de seguridad*. En la fase de penetración, los hackers pueden correr scripts o programas en contra de los servidores y ponerse ellos mismos en una posición donde puedan ganar acceso hacia el sistema. Con muchos de los gusanos populares de los últimos años, los atacantes buscaban causar sobre flujos del buffer (el cual permite a un atacante el sobrescribir la memoria con su propio código). Y entonces ejecutar un programa shell desde el buffer, ganando acceso en modo shell con derechos administrativos para atacar la máquina. En muchos casos, los hackers literalmente tienen un prompt DOS desde una maquina atacada que esta desplegado en los dispositivos que estos usan para lanzar el ataque.
3. **Persistencia:** después de que los atacantes tienen el control de una maquina, estos pueden descargar software malicioso y quizás instalarlo en el directorio del sistema o ponerlo en el arranque del sistema de la maquina atacada, de esta manera aun si la maquina atacada es reiniciada los hackers todavía tienen el control de la maquina. Durante esta fase, los atacantes pueden agregar usuarios y passwords por lo tanto estos pueden fácilmente regresar a

la maquina cada vez que quieran. Los atacantes en este punto tienen el control sobre el dispositivo, y debido a que el dispositivo esta en la red, estos pueden elegir atacar otros dispositivos dentro de la red, estos puede elegir atacar otros dispositivos o usar un sniffer de red para robar nombres de usuarios y los passwords desde otros dispositivos.

4. **Propagación:** en esta fase, el código malicioso corrido en la fase de persistencia busca otras maquinas con la misma vulnerabilidad para atacarlas e infectarlas usando el mismo procedimiento y código malicioso. El gusano llamado Slammer hizo de esto algo extremadamente efectivo, infectando 1.4 millones de host en un lapso de tiempo muy pequeño. La mayoría de los atacantes publicados en los años pasados (incluyendo gusanos como slammer, código rojo, nimda, sasser y blaster) han tenido una fase de propagación exitosa.
5. **Paralizar:** esta es potencialmente la etapa más dañina de un ataque. El objetivo o efecto colateral de muchos gusanos es usar hasta el máximo de todo el ancho de banda y poner todas las redes de la corporación como inutilizables. Sin embargo, otros gusanos son mas destructivos y remueven los archivos claves (causando de que los sistemas colapsen), para crear puertas traseras o robar información del cliente, entre las cuales se tienen tarjetas de créditos, listas de clientes o información financiera. Es de imaginar por un segundo todo el daño que pudo haber sido hecho por un gusano como lo es slammer. Si el autor hubiese elegido el buscar en un disco duro y robar números de tarjetas de crédito en todas las computadoras comprometidas, en vez de inundar toda la red, potencialmente hubiesen sido diez mil tarjetas de crédito las que se hubieran usado para actividades fraudulentas y no hubiesen costado a los negocios y los consumidores millones de dólares.

Este modelo de ataque fue utilizado en el primer ataque a una red (el gusano morris, 1988) y aun en día es utilizado. Este modelo es un ataque de gusano clásico. Virus por email y ataques dirigidos usan básicamente el mismo método, excepto que la fase de prueba no es generalmente necesaria antes del ataque del virus.

c. Eligiendo las víctimas

En muchos casos, excepto por venganza o fama, los hackers seleccionan a sus victimas aleatoriamente, buscando sistemas fácilmente de atacar. Si encuentran una red en cual es fácil entrar, estos se aprovechan de esto y comienzan a atacar esa red. Si el hacker trata de penetrar en un sistema y no puede obtener información básica, en muchos casos, estos se dan por vencidos después de pocos intentos. Sin embargo, no hay que confiarse en esto para proteger la red. Es importante poner seguridad punto a punto penetrante en lugar de solo defenderse contra un ataque en caso de que el hacker no se rinda y encuentre una vulnerabilidad.

Los hacker corren analizadores de vulnerabilidades de red por muchos días y terminan usando muchas direcciones IP diferentes. Cuando el software reporta una vulnerabilidad que estos pueden atacar, su blanco es identificado. El software de análisis provee la siguiente información:

- Un reporte de cuales servicios o puertos han sido pasados a través del firewall en la red que han analizado.
- Un reporte de los sistemas operativos usados en los puertos abiertos.
- Un reporte de las aplicaciones usadas en el puerto abierto.
- El reporte más alarmante, un reporte en el cual las vulnerabilidades son mostradas mediante la combinación del sistema operativo y la aplicación.
- La información que necesitan para descubrir como atacar la vulnerabilidad y llegar al sistema.

El mensaje es que cualquier compañía o persona que esta conectada al Internet puede ser victima de un ataque aleatorio por parte de un hacker.

2.3.2.1. El Hacker.

El término hacker se refiere a programadores y no a los que practican una abertura ilegal en la seguridad de sistemas. Un hacker es cualquier persona que investiga la integridad y la seguridad de un sistema operativo. La mayoría normalmente, son

individuos programadores. Usualmente han adelantado sus conocimientos en hardware y software para utilizar los sistemas de una forma innovadora.

Los hacker´s determinan a menudo nuevas maneras de utilizar o de poner a prueba una red en ejecución, de una forma en que los fabricantes de software no habían pensado.

Entre los hacker´s mas conocidos tenemos:

Dennis Ritchie, Ken Thompson, y Brian Kernighan: Ritchie, Thompson, y Kernighan son programadores en Bell Labs, ellos son los padres del lenguaje de programación C. Además escribieron un sistema operativo muy flexible y potente en el cual se basaría Linux. Dentro de ese grupo, hace su aparición un hombre que podríamos llamarlo el padre del Movimiento del Software Libre. Richard M. Stallman. Creador del Free Software Foundation (Fundación de Software Gratuito). Estas personas todavía se mantienen ocupadas por ejemplo: Ritchie está ocupado dedicándose al Plan nueve del Bell Labs. Es un sistema operativo nuevo que probablemente suplantará UNIX.

Richard Stallman: se unió al Instituto tecnológico del Laboratorio de inteligencia artificial de Massachusetts en 1971. entre los premios recibidos están: el ACM Grace Hopper, una membresía en la MacArthur Foundation, el Pioneer Award de la Electronic Frontier Foundation y el Takeda Award por mejoras político/sociales, así como varios doctorados honoríficos. Finalmente creo la Fundación de Software Gratuito, que generá servicios públicos de libre distribución y programas para el uso de plataforma UNIX. Trabajó en algunas máquinas arcaicas, para cuál probablemente todavía tiene acceso a ciertas parte. Él es uno programador genial.

Tim Bernes Lee y Vinton Cerf: concibieron una red abierta, donde el conocimiento sería totalmente libre. Vinton Cerf es el inventor de los protocolos TCP/IP.

Paul Baran, Baran: es probablemente al máximo hacker de todos ellos por una razón: Él estuvo enredado con el Internet incluso antes de que existiera. Baran comenzó a edificar lo que es hoy día, un navegador. La cual millones de internautas la utilizan a diario.

Eugene Spafford Spafford: es un profesor de informática, famoso por su trabajo en Purdue University. Él fue creador de la Contraseña del Computadora Oracle y de Sistemas de seguridad, un sistema semiautomatizado para asegurar la red.

Linus Torvalds: uno de los individuos mas extraordinario, Torvalds se enroló en las clases de UNIX y en el lenguaje de programación C en los inicios de 1990s. Un año más tarde, empezó a escribir un sistema operativo análogo a UNIX. Dentro de un año, él lanzó al mercado este sistema para el Internet (fue llamado Linux). Hoy, Linux tiene un culto que es la distinción de ser el sistema operativo desarrollado por programadores del software en todo el mundo entero. Linux está libre de restricciones de derecho de autor y está disponible gratuitamente para alguien con acceso al Internet.

Bill Gates y Paul Allen: desde sus días en la escuela secundaria, estos hombres de Washington hacían software. Ambos son programadores expertos. Empezaron 1980, construyeron lo más grande y el imperio del software más exitoso en la tierra. Sus éxitos comerciales incluyen MS-DOS, microsoft windows 95 y windows NT.

Grace Hooper: se graduó en matemáticas y física en el Vassar College. Completó su maestría y doctorado en la universidad de Yale y durante la segunda guerra mundial se alistó en la marina de Guerra de los Estados Unidos, llegando a ascender al grado de Almirante. Creó el lenguaje Flowmatic, con el cual desarrolló muchas aplicaciones y en 1951 produjo el primer compilador, denominado A-0 (Math Matic). En 1960 presentó su primera versión del lenguaje COBOL (Common Business-Oriented Language). Para muchos estudiosos, la almirante Grace Hooper es considerada la primera hacker de la era de la computación

Adrian Lamo: el hacker sin hogar, y mas famoso del mundo duerme por lo general en un edificio en construcción cerca de Ben Franklin en Philadelphia y cuando despierta se dirige a una computadora pública con conexión al Internet, con el objetivo de espiar entre los servidores del Internet. Sin embargo lleva siempre consigo una laptop Toshiba y un celular, en caso de no encontrar un sitio disponible.

Lamo trabaja temporalmente como consultor de seguridad, a pedido de corporaciones de trabajadores independientes (freelance). El pasado Enero del 2003 encontró un fuga en la red hermética de la corporación Excite@Home.

Este joven de 21 años manifiesta que está ayudando a las compañías y a los usuarios a entender los límites de la seguridad en Internet, aunque sus métodos alarmen a los gigantes del medio.

Hace 2 años, Lamo se hizo conocido en los círculos de hackers al haber ingresado en las redes de América on Line, Yahoo y Worldcom, informando a sus administradores la forma cómo lo hizo. Los propios administradores lo han llamado brillante debido a que con mucha habilidad descubrió estos huecos en sus redes. Los críticos califican a Lamo como un charlatán que quiere llamar la atención. ¿"Está alguien impresionado con las habilidades de Lamo? Él no está haciendo nada que sorprenda particularmente. Tampoco ha descubierto un nuevo concepto de la seguridad. Él está buscando los huecos básicos" escribió un miembro del foro de SecurityFocus.

Lamo encontró una vulnerabilidad en la red del periódico The New York Times en menos de dos minutos. "Es tan simple a pesar de que muchos se consideran un cinturón negro de las artes marciales de las computadoras". A pesar de sus buenas intenciones, Lamo podría ir a la cárcel por lo que está haciendo. Lo curioso del caso es que hasta ahora nadie lo ha acusado formalmente.

2.3.2.2 Los cracker.

Los cracker son individuos quiénes usan el conocimiento del Internet y de la computación para comprometer la seguridad de la red. Históricamente, esta actividad involucra una gran variedad de técnicas para robar archivos encriptados o para lograr sus objetivos. Para diferenciar entre estos dos grupos, simplemente recuerde esto: Los cracker´s se involucran en actividades sin autorización para violar la seguridad de una red.

¿Por qué existen los cracker?

Los cracker existen por condición necesaria. Porque la naturaleza humana está ni más ni menos, conducida por un deseo de arruinar en lugar de crear. El único asunto aquí es de qué tipo de cracker hablamos. Algunas cracker para beneficiarse se colocan un título lucrativo. Estos pueden aterrizar en un campo de batalla, entre dos compañías que luchan por ganar el mercado, un ejemplo seria:

- Compañía A: Coca Cola
- Compañía B: Pepsi Cola
- Objetivo: luchar por sacar de la red el servidor Web de una de las dos compañías.

Hay cracker de alquiler que Quebrarán cualquier tipo de sistema, por un precio. Como por ejemplo: recuperar la lista de perfiles de un banco. Existen cracker´s que son niñas que demuestran una habilidad extraordinaria para entender altamente el conocimiento técnico de las computadoras. Otras persecuciones comunes son: las clonaciones de teléfonos celulares, esquemas de piratería y fraude.

Con la presente documentación se quiere dejar claro que cualquier tipo de cracker`s de ser encontrados culpables del delito cometido podrían pagar grandes condenas en prisión.

Entre los cracker´s mas conocidos tenemos:

Kevin David Mitnick: es el más famoso crackers de los últimos tiempos. Nacido el 6 de agosto de 1963 en Van Nuts, California. Desde muy niño sintió curiosidad por los sistemas de comunicación electrónica y fue cultivando un obsesivo deseo por investigar cosas y lograr objetivos aparentemente imposibles, hasta llegar a poseer una genial habilidad para ingresar a servidores sin autorización, robar información, interceptar teléfonos, crear virus, etc.

Cuando en 1992 el gobierno acusó a Kevin de haber substraído información del FBI, relacionada a la investigación de Ferdinand Marcos y de haber penetrado en computadoras militares, el se convirtió en un símbolo entre la comunidad internacional de crackers.

Mitnick fue arrestado por el FBI en Raleigh, North Carolina, el 15 de Febrero de 1995, y fue liberado en Enero del 2000, después de permanecer casi 5 años en una prisión federal, le costó al estado norteamericano y a la empresas privadas, millones de dólares al ser objeto de hurto de software, información y alteración de los datos de las mismas. Entre los agraviados se incluyen corporaciones tales como Motorola, Novell, Nokia y Sun Microsystems, el FBI, el Pentágono y la universidad de Southern California.

Kevin Poulsen: habiendo Seguido un camino muy parecido a Mitnik, Poulsen es más conocido por su extraña habilidad para agarrar control del sistema telefónico de pacific Bell. Poulsen una vez usó este talento para ganarse un certamen radiodifusor donde el premio fue un Porsche. Poulsen también ha quebrantado casi cualquier sitio, pero tiene una inclinación especial por sitios conteniendo datos de defensa. Esto ocaciono en el último período una en cancelación que duró cinco años. Poulsen fue soltado en 1996 y aparentemente se ha reformado.

Justin Tanner Peterson: conocido como Agente Steal, Peterson es probablemente más famoso por manipular una agencia prominente de crédito al consumidor.

Peterson pareció estar motivado por dinero en lugar de la curiosidad. Esta falta de filosofía personal condujo a su caída y la caída de otros.

Vladimir Levin: graduado en matemáticas de la universidad Tecnológica de San Petesburgo, Rusia, fue acusado y preso por la Interpol después de meses de investigación por ser la mente maestra de una serie de fraudes tecnológicos que le permitieron a él y la banda que conformaba, substraer más de 10 millones de dólares, de las cuentas corporativas del Citibank. A pesar de que la banda substrajo más de 10 millones de dólares al Citibank, Levin fue sentenciado a 3 años de prisión y a pagar la suma de US $ 240,015 a favor del Citibank, ya que las compañías de seguros habían cubierto los montos de las corporaciones agraviadas. Vladimir Levin ahora se encuentra en libertad.

Chen Ing-Hou: es el creador del virus CIH, que lleva sus propias iniciales. Manifiesta que siente mucho por tanto daños causados, pero que ello fue motivado por una venganza en contra de los que llama "incompetentes desarrolladores de software antivirus". Chen Ing-Hou nació en la ciudad de Kaohsiung, en Taipei, capital y principal ciudad de Taiwan, y creó su famoso virus en Mayo de 1998, al cual denominó Chernobyl, en conmemoración del 13 aniversario de la tragedia ocurrida en la planta nuclear rusa. Actualmente trabaja como experto en Internet Data Security.

2.3.3. La persona de negocio.

La persona de negocio se refiere a cualquier individuo que ha establecido o establecerá una empresa mercantil que usa la red como un medio para realizar sus transacciones. Por lo tanto, una persona comercial dentro del significado utilizado en esta tesis: es alguien que transmite comercio por la red ofreciendo bienes o servicios. Nota: No tiene importancia si estos bienes o estos servicios son ofrecidos gratuitamente como un servicio promocional.

2.3.4. El periodista.

Un periodista es una persona que se encarga de reportar o cargar en una cuenta de Internet toda la información recolectada. Éste puede ser alguien que trabaje en enviar noticias por medio del correo electrónico o un estudiante de educación superior escribiendo para su periódico universitario. La clasificación no tiene nada que ver con cuánto dinero está pagado por la información, ni en dónde la información es publicada.

2.3.5. El usuario informal.

Un usuario informal es un individuo quien usa el Internet puramente como una fuente de entretenimiento. Tales usuarios raramente gastan más de diez horas a la semana en la red. Se deslizan sobre temas que son de interés meramente personal.

2.3.6. El especialista en seguridad.

Un especialista en seguridad es alguien encargado de asegurar una o más redes de ataques. No es necesario que reciban pago por sus servicios a fin de calificar en esta categoría. Algunas personas hacen esto por afición. Si lo hacen, son especialistas.

2.4. ¿ES LA SEGURIDAD UN ESFUERZO INÚTIL?

El equilibrio del conocimiento se mantiene en los cracker's como una constante a sólo pulgadas atrás de los hacker's. Algunos escritores afirman que a lo largo de este proceso, una forma de evolución de hacker's esta ocurriendo, queriendo decir que los cracker's finalmente serán descalificados y que muchos irán a las cárceles, otros se pondrá mayores y más sabios, y así sucesivamente. Pero esto es probablemente poco realista.

Desde el primer escrito de Paul Baran, la seguridad en el Internet ha sido una preocupación. A lo largo de los años, la seguridad por ambigüedad se ha convertido en la actitud predominante de la comunidad informática.
Los siguientes principios:

- Si no habla estará bien.
- Si se esconde quizás no lo encuentren.
- Si la tecnología es compleja; usted está a salvo.

Se han probado que no son correctos, además van en contra de los conceptos originales de cómo podría evolucionar la seguridad a través del debate y la educación. La discusión abierta sobre estándares y metodologías fue sugerida fuertemente con el fin de fomentar avances importantes en la tecnología.

Baran estaba bien consciente de esto y en un articulado fundamental escribió: Sin la libertad para dar a conocer la propuesta del sistema difundido por mentes listas de intereses diversos, es aumentar los riesgos significativos de los puntos débiles que han sido pasados por alto.

2.4.1. La seguridad a través de la oscuridad.

La seguridad a través de la oscuridad ha estado definida y descrita de muchas formas diferentes. Una descripción caprichosa, publicada por Jeff Breidenbach se detalla a continuación: “la red tenía una estrategia brillante llamada: seguridad de la red a través de la oscuridad. la cual permitía que cualquier persona le engañaran el pensamiento de que esto fue hecho a propósito. Además el software ha crecido en un lío tan enredado que nadie realmente sabe utilizarlo. Debido a que los mismos ingenieros están aturdidos mentalmente y esperando que los intrusos potenciales estén tan intimidados por los detalles técnicos como ellos mismos”.

El Sr. Breidenbach bien podría estar en lo correcto acerca de esto. Sin embargo, la descripción y definición estándar de seguridad a través de la oscuridad puede variar

dependiendo la fuente, ya que se puede obtener de cualquier archivo disponible en millares de sitios del Internet. El concepto que se utilizara es el siguiente: se denomina así a la seguridad que se basa en el desconocimiento y el ocultamiento de fallas, en lugar de preverlas y solucionarlas.

Grandes compañías y gobiernos en todo el mundo se empeñan en perseguir la seguridad a través de la oscuridad: consideran que ocultando los detalles de cómo funcionan sus algoritmos conseguirán aumentar la seguridad global de sus sistemas. Nada más lejos de la realidad. En estas situaciones, lo que inevitablemente ocurre es que el desarrollo de los algoritmos de protección de la confidencialidad se deja en manos de un equipo de ingenieros y técnicos que lo llevan a cabo de la mejor manera que saben y que, sin duda alguna, superan con éxito los ataques convencionales, ofreciendo una seguridad satisfactoria a primera vista.

Sin embargo, para contar con mayores garantías de que un algoritmo o protocolo es seguro, no basta con que sea revisado por un conjunto de personas en seguridad, es necesario someterlo al público para reunir un equipo de investigación de cientos o miles de expertos que trabajarán durante meses o años en la búsqueda de fallas y vulnerabilidades.

A pesar de cualquier filosofía en seguridad, tres preguntas permanecen constantes:

- ¿Por qué el Internet es inseguro?
- ¿Necesita ser seguro?
- ¿Puede ser seguro?

2.4.2. ¿Por qué es el Internet inseguro?

El Internet es inseguro por una variedad de razones, que se discutirá aquí detalladamente.

- La falta de educación.

- El diseño del Internet.
- El filtro de la tecnología.
- La naturaleza humana.

Cada uno de estos factores contribuyen hasta cierto punto a la falta de seguridad en el Interne.

a. La falta de educación:

¿Cree usted que lo que usted no sabe no puede lastimarlo? Si usted es acusado de correr un servidor, entonces consideraría que la educación es la única razón importante en la seguridad, aunque ha sido severamente deficiente en los últimos tiempos.

No se expone que exista una falta de educación dentro de instituciones de alto aprendizaje o en organizaciones que realizan tareas orientadas a la seguridad. Más bien, se propone que la educación en seguridad se extienda más allá de esos grandes baluartes conocedores de la ciencia en seguridad informática.

El Computer Emergency Response Team (CERT) es probablemente la organización mas conocida en la seguridad del Internet. El CERT genera anuncios sobre seguridad y los distribuye lo largo de toda la comunidad del Internet. Estos anuncios contienen lo último sobre los sistemas operativos conocidos y sus vulnerabilidades en la seguridad. El CERT de esa manera realiza un servicio sumamente valioso para el Internet.

El CERT es un centro de coordinación, establecido por la agencia de investigación avanzada de proyectos (ARPA) en 1988. Provee un punto centralizado para la denuncia y reacciona de una forma anticipada a los incidentes principales de seguridad.

Referencia: se puede contactar con el CERT en su página http://www.cert.org. Allí reside una base de datos de vulnerabilidades en la red, papeles de diversas

investigaciones incluyendo documentación extensiva sobre supervivencia en desastres y enlaces para otros recursos importantes acerca de la seguridad.

Existen muchos informes estadísticos en el CERT acerca de los sitios que han experimentado alguna violaron en su seguridad o de actividades sospechosas. Esto podría ser porque la mayoría de servidores en el Internet están mantenidos por personas que tienen poca educación en seguridad. Existe mucha información de seguridad disponible en el Internet que apunta hacia el CERT, pero estas pueden aparecer inicialmente auto conduciéndonos a noticias para seguridad.

De 1991 hasta ahora, el foro de seguridad ha sido un excelente lugar para empezar. Como la tecnología del Internet crece de una manera acelerada, algunos textos se desfasan rápidamente. De igual forma, el nuevo administrador de sistemas debe mantenerse informado con cada tecnología de seguridad que va surgiendo. Hacer esto es una tarea difícil.

- **Diseminación de información**

Por tantas razones, la educación en seguridad esta deficiente. En el futuro, los especialistas necesitan tratar esta necesidad de una manera más práctica. Deben de haber algunos medios convenientes para conectar esta información a la red. Algunas organizaciones hacen un llamado a hacer esto, pero muchas son forzadas a cargar altos precios por sus bases de datos. The National Computer Security Association (NCSA) es: una de de estas organizaciones que aproximadamente recolecta 70MB de información en seguridad diarios. Su base de datos es investigable y está disponible por un precio muy bajo.

Muchas organizaciones ofrecen capacitaciones en seguridad y en tecnología. El precio por estas capacitaciones varían, dependiendo de la naturaleza del curso,. Una buena fuente de guía es Lucent Technologies, que ofrece muchos cursos de seguridad. Pero a pesar de la disponibilidad de tales guías, las compañías se encuentran todavía sin ninguna referencia para buscar esa información valiosa sobre seguridad.

En realidad, el porcentaje de compañías que mantienen seguras las redes es muy bajo además están como que algo lejos de la realidad. Una conducta más observadora de parte del instituto de seguridad computacional encontró que más del 50% de los participantes observados nunca escribieron sobre políticas o procedimientos de seguridad.

- **Los problemas con una PC basada en sistemas operativos.**

Debería ser notado que en América el incremento en los servidores ha ido creciendo por nuevas posturas del internet, adicionando nuevos problemas en la educación. Muchos de estos individuos han usado sistemas basados en PC llegando a la conclusión que nunca fueron diseñados para asegurar las operaciones en la red.

Tradicionalmente, los usuarios de PC's han tenido poco contacto con los vendedores, excepto en problemas relacionados a la configuración del hardware y software. Pero esa no es su culpa.

Los programadores suelen ser brillantes en la codificación y el diseño de sus aplicaciones para usuarios finales pero tienen un pobre conocimiento en seguridad. La comunidad de PC's en cierta medida no le interesa la seguridad, ellos tienen un mercado basado en una estrategia donde los vendedores venden el concepto de usuarios contentos, conveniencia, y estandarización de aplicaciones.

Los programadores pueden tener algún conocimiento de seguridad pero son incapaces de implementarlas porque no pueden anticipar ciertas variables. Foo (la variable) en este caso representa las innumerables diferencias y dificultades envueltas con las otras aplicaciones que se ejecutan en la misma maquina.

Existen muchas variables diseñadas por diferentes individuos y vendedores, que son desconocidas por los programadores. Esto no es inusual para la combinación de dos terceras partes de los productos, pero resultan en el compromiso parcial de la seguridad del sistema. Similarmente, aplicaciones creadas para proveer seguridad pueden, corren en plataformas de PC, deteriorando de otra forma la seguridad.

El típico ejemplo es el uso de la famosa utilidad de encriptación Pretty Good Privacy (PGP) cuando se usa en el ambiente de Microsoft Windows. PGP opera aplicando un complejo algoritmo. Estas operaciones resultan de muy alto nivel de encriptación. En algunos casos, si el usuario lo especifica, usando PGP puede producir encriptación de nivel militar para el usuario del hogar.

Si el dato es encriptado puede ser desencriptado, alterado, o de otra manera accesado por personas no autorizadas. PGP opera en una interfase de línea de comando o de un prompt DOS. Esto en si no presenta un capitulo de seguridad. El problema es que mucha gente encuentra esto como un inconveniente y se ven forzados a usar un interfaz, o una aplicación de Microsoft Windows a través de la cual puedan acceder a rutinas PGP. Cuando el usuario hace uso de la interfaz, la frase clave es escrita dentro de un archivo swap de Windows. Si ese archivo swap es permanente, la frase clave puede ser rebotada usando maquinas relativamente potentes. Se ha experimentado con maquinas con diferentes configuraciones. Con un archivo swap de 20MB en una IBM compatible DX66 sporting 8-16MB de RAM, esta es una formidable tarea que prácticamente “traba” la maquina. Esto, también, depende de la aplicación que se este utilizando para hacer la búsqueda. La aplicación más efectiva para realizar una búsqueda es el GREP.

Hay versiones gratuitas de GREP disponibles en el Internet para una variedad de sistemas operativos, incluidos pero no limitados para UNIX, DOS, OS/2, y 32- bit en ambiente Microsoft Windows.

En cualquier evento, el factor dificultad cae drásticamente cuando usas una maquina con recursos superiores a 100MHz y 32MB de RAM. El punto es este: no es culpa de los programadores del PGP que las frases claves sean atrapadas en el swap. PGP no es un fallo, ni lo son esas plataformas con memoria swap. No obstante, plataformas que usan memoria swap no están seguras y probablemente nunca lo estén.

Cuando los programadores diseñan productos de seguridad, suelen enfrentarse con problemas inesperados sobre los que ellos no pueden ejercer control. Las técnicas de programación seguras ayudan a los programadores a no debilitar la red y a solucionar algunos problemas en la seguridad del software.

b. El diseño del Internet.

Cuando los ingenieros se vieron obligados a la tarea de crear el internet de una manera abierta, fluida y accesible se lo tomaron con mucha alegría y entusiasmo ya que el proyecto era demasiado potente. La Internet es la creación más notable y admirable construida por el género humano. Hoy en día existen muchas maneras de conseguir información relacionada con diversos temas en el Internet; hay docenas de protocolos con los cuales se puede hacer entre ellos: FTP, http, BBS basado en telnet, un GOPHER, NFs cSmb y la lista continua. Cada uno de estos protocolos forma un aspecto del Internet moderno. Además representa una pequeña red de si misma. Cualquier maquina corriendo implementaciones modernas de TCP/IP pueden utilizar todos estos y mas.

Las redes heterogéneas fueron una vez un sueño. Ahora son una confusión y un desorden de redes alrededor del mundo. Los expertos en seguridad han tenido por años que correr de un lado para otro antes de detener la información y los protocolos para tapar los agujeros en sus sistemas o aplicaciones debido a los crackers.Los cracker`s vienen con un armamento pesado, para detectar el flujo o violar toda la seguridad de aquí, de allá o de cualquier lado. Parte del problema es en el diseño básico del internet.

Tradicionalmente, la mayoría de los servicios en el Internet se encuentran con el modelo client/server. Esta situación no se ve que cambie en un futuro cercano. Hoy en día, la programación client/server es la habilidad mas buscada porque trabaja con eficacia, y no hay reemplazo viable con respecto a este punto. La tarea de un cracker`s, por lo tanto, esta limitada en una sola razón: ir al corazón del servicio y quebrar al servidor.

Existen otros problemas asociados con el diseño del internet, específicamente relacionados a la plataforma UNIX los cuales son: el control de acceso y el de los privilegios. En UNIX, cada proceso tiene un nivel de privilegio como mínimo, es decir privilegio para acceder a los archivos o a los directorios donde se encuentran los archivos depositados, procesos comunes y programas que están ya configurados predeterminadamente.

Más allá de esto, un administrador de sistemas puede determinar el plan de acción específicamente para determinar los privilegiados, dependiendo de la necesidad de la situación. El administrador de sistema ofrece una amplia variedad de opciones al respecto. En resumen, los administradores de sistemas son capaces de restringir uno, cinco o 100 personas. Además, estas personas o grupos de personas pueden estar también limitados a ciertos tipos de acceso, como leer, escribir, ejecutar, y así sucesivamente.

Unix es uno de los sistemas mas completos, por lo tanto se requiere experiencia en la parte administrativa. El sistema provee cierto riesgo de seguridad inherente. Uno de los riesgos es: el acceso que garantiza privilegios a procesos o a los usuarios que están permitidos incrementar su acceso mas allá de lo que tienen originalmente asignado. Por ejemplo, una utilidad que requiere cualquier forma de acceso primario (alto nivel de privilegio) podría ser visto como precaución. Si alguien encuentra un fallo con ese programa y puede efectivamente explotar eso, la persona ganara un alto nivel de acceso.

Nota: El acceso de control ha sido integrado dentro del sistema operativo Windows NT por lo tanto, el fenómeno no es exclusivamente relacionado a UNIX. Novell NetWare también ofrece algunos rasgos bastante fuertes de control de acceso.

Todos esos factores influyen seriamente el estado de seguridad del Internet. Claramente cientos de pequeñas cosas se conocen acerca de esto. Esto implica que un buen administrador de sistemas puede idealmente tener conocimientos de por lo

menos tres plataformas. Esto nos trae a otra consideración: ¿Porque el diseño del Internet es tan complejo?

Hay otros aspectos del diseño y composición del Internet que los autores suelen citar como fuentes de inseguridad. Por ejemplo, la red permite una cierta cantidad de anonimato. En cierta mediad es bueno que los individuos que necesitan comunicarse de una forma anónima puedan hacerlo tantas veces sea la necesidad.

- **Anonimato en la red.**

Hay muchas razones para utilizar la comunicación anónima. Una razón es que las personas que viven en estados totalitarios pueden contrabandear noticias sobre violaciones a los derechos humanos. Por lo menos, esta razón es sacudida regularmente alrededor de tantas personas que se encuentran en los medios. Aunque el porcentaje de la gente que usa el Internet para esta noble actividad es increíblemente pequeña. Sin embargo, no hay necesidad de proporcionar las excusas del porqué el anonimato, si existe el Internet. Después de todo, no hay una razón por la que las personas deban de ser prohibidos de hacer algo en una red pública que pueda ser legal en cualquier otro lugar. Si los seres humanos desean comunicarse anónimamente, es su derecho.

Mucha gente usan los remailers para poderse comunicar anónimamente. Éstos son servidores configurados para aceptar y remitir los mensajes del correo. Durante este proceso, la cabecera y la dirección de origen son quitadas del mensaje, de tal modo que se cubre al autor y su localización. En su lugar se inserta la dirección del remailers anónimo.

Los mailers anónimos han sido el tema de controversia en el pasado. Mucha gente, particularmente miembros de entidades muy prestigiosas, sienten que los remailers minan la seguridad del Internet. Algunos describen la situación como obscura y que cada día se va poniendo peor. La introducción de mailes anónimos en el Internet ha alterado la capacidad de balancear ataque y contraataque, o crimen y el castigo Pero la verdadera amenaza más grande para la viabilidad comercial, económica y

política de la infraestructura de información global vendrá de terroristas de la informática.

Sin embargo, se ven periodistas hacer declaraciones, tales como ésta por Walter S. Mossberg: “en muchas partes del dominio digital, usted no tiene que utilizar su nombre verdadero. Es a menudo imposible calcular la identidad de una persona que hace demandas políticas “.

Esto es una declaración interesante. Por muchos años, El Tribunal Supremo ha sido indiferente al requerir que las declaraciones políticas sean acompañadas por la identidad del autor. Esta denegación es asegurarse de que el discurso libre no está silenciado.

El anonimato del E-mail en el Internet tiene un efecto insignificante en aplicaciones verdaderas a la seguridad del Internet. Los días cuando uno podía explotar un agujero enviando un mensaje simple del E-mail se han ido hace tiempo. Sin embargo el anonimato de E-mail es una adición de todos, está para los de seguridad nacional

- **Propietariado**

Antes de comenzar se debe definir esté término. Propietariado es: una práctica emprendida por los vendedores comerciales quienes procuran inyectar dentro del Internet varias formas de diseño propietario. Haciendo esto, ellos esperan crear los beneficios en un ambiente que ha estado previamente libre de reinado comercial. Interfiriendo con la estructura de la seguridad del Internet y derrotando la capacidad del Internet para servir a todos los individuos igualmente y con la misma eficacia.

- **ActiveX**

Un buen ejemplo de propietariado es: la tecnología ActiveX de Microsoft Corporation's.

Referencia: los usuarios que desconocen la tecnología de ActiveX deben visitar la pagina:http://www.microsoft.com/activex/. Los usuarios que tienen ya cierta

experiencia con ActiveX deben ir directamente a la página de Microsoft que trata sobre las características de la seguridad: http://www.microsoft.com/security/.

Para entender el impacto de ActiveX, es necesario conocer un poco acerca del HTML. El HTML era una brecha increíble en la tecnología del Internet. Con forme el paso del tiempo se fueron utilizando herramientas importantes hasta llegar a la actual que son: los protocolos. Estos ayudan al usuario en cualquier lado, en cualquier máquina, que se encuentren ver información y esa misma, ser vista bastante igual por otro usuario en otro lugar del mundo.

La tecnología de ActiveX es un nuevo método de páginas. Se diseña para interconectar con el Internet Explorer. Si usted no lo tiene, olvídese de él. Porque La mayoría de las páginas www son diseñadas para que utilicen el Internet Explore. Esa situación puede cambiar, porque Microsoft está empujando para que las extensiones de ActiveX sean incluidas dentro del proceso de la estandardización del HTML. Sin embargo, tales extensiones compiladas alteran el estado de la seguridad del Internet de una manera amplia.

Para examinar el problema a fondo de los ActiveX se puede visitar la página establecida por Kathleen A. Jackson, líder del equipo, la oficina de seguridad de la división, computando información, del laboratorio nacional de Los Alamos. Los puntos de Jackson para afinar los problemas en los ActiveX los describe de la siguiente manera:

- Se introducen las nuevas tecnologías que son propietarias. Estas tecnologías debido a que son propietarios no se pueden examinarse de cerca. Por otra parte, estas plataformas no son cruzadas y por lo tanto no crean limitaciones en la red, en comparación con soluciones heterogéneas.
- Un problema grande con los ActiveX es la seguridad. Un programa que se descarga puede hacer cualquier cosa que el programador desea. Puede formatear su disco duro o cerrar su computadora.

Cuando Microsoft fue alertado del problema, la solución fue reclutar a una compañía para crear las firmas digitales de los controles activeX. Esta firma digital se supone que fue firmada por el programador o el creador del control. La compañía responsable por esta firma digital tuvo como señal la promesa de los editores de software, la cuál es un acuerdo de no firmar ningún software que contenga código malévolo. Si un usuario navega en una página que contenga un control sin firmar, El Internet Explorer de Microsoft pone una caja de mensaje de alerta diciendo si usted desea aceptar el control sin firmar digital.

No nos podemos imaginar que tan absurdo parece para los profesionales de la seguridad, estar cada momento evitando el código malévolo, firmado o sin firmar, en cualquier Sitio Web, y si se firma, que garantías hay que el controlador sea seguro. Esto no es practico y además es poco realista.

Microsoft y la compañía responsable de la iniciativa de firma ofrecerán fácilmente aseguramientos, qué evidencia que tales firmas no pueden ser forjadas. Existe la incomodidad para los programadores de ciertas firmas de controles, cuántos usuarios rechazarán o aceptaran un control sin firmar. La mayoría de los usuarios enfrentados con el mensaje de advertencia no tienen ninguna idea de qué significa. Todos lo que representa para ellos es una obstrucción que está evitando que entren a una página Web.

Pocos han probado de verdad la seguridad. Esto llegará a ser más frecuente y, para el crédito de Microsoft, La tecnología de ActiveX crea las páginas más imponentes de WWW disponibles en la red. Estas páginas han aumentado funcionalidad, incluyendo cajas drop-down, menús, y otras características que hacen que navegar en el Web sea un placer.

Referencia: Para mejorar los conocimientos acerca de la estandardización del HTML, visite el sitio del consorcio del World Wide Web (http://www.w3.org). Si usted desea ya puntos específicos sobre las etiquetas y de extensiones del HTML, usted debe

leer la declaración de la actividad de W3C's en esta edición http://www.w3.org/pub/WWW/MarkUp/Activity.

Propietariado es una fuerza peligrosa en el Internet, y está ganando terreno rápidamente. Para componer este problema, algunos de los productos propietarios son excelentes. Por lo tanto es perfectamente natural que los usuarios se cambien hacia estos productos. Los usuarios estan mas interesados de la funcionalidad y no de la seguridad. La responsabilidad está en los vendedores, y esto es un problema. Porque los vendedores tienen que hacer mas conciencia sobre los peligros de la seguridad. Uno no puede, por ejemplo, prohibir los productos inseguros que se encuentran en el mercado.

Los vendedores tienen ciertamente el derecho de lanzar cualquier software que ellos quieran en el presente, seguro o no. Por lo tanto, no hay solución a este problema. Extensiones, idiomas, o las etiquetas que autorizan probablemente incluyen la examinación de un:

- JavaScript
- VBScript
- ActiveX

El Javascript es poseído por Netscape, VBScript y ActiveX son poseídos por Microsoft. Estos lenguajes son las armas de la guerra entre estos dos gigantes. Se duda que ambas compañías tengan como objetivo la necesidad de tener ambas tecnologías. Por ejemplo, Netscape no puede sacudirse la presencia de Microsoft en el mercado de escritorio. Igualmente, Microsoft no puede proveer al mundo de UNIX con sus productos. El Internet se beneficiaría probablemente si estos dos titanes enterraran el hacha de guerra detrás de cada uno.

c. El filtro de la tecnología

El problema de la tecnología de alto nivel es que es filtrada primero por militares, científicos, instituciones que se encargan del buen estado del Internet como son:

IEEE (instituto de ingenieros eléctricos y electrónicos), ANSI (Instituto Nacional Americano de Normalización), TIA (Asociación de la Industria de Telecomunicaciones) y la EIA(la Asociación de la Industria Electrónica),Y posteriormente pasa a formar parte de toda la comunidad del Internet.

Las empresas a menudo suministran vínculos informativos sobre herramientas avanzadas en seguridad. En algunos sitios la información sobre las herramientas de seguridad es gratis y de muy buen contenido referente a o lo ultimo en el mercado. Además de estas empresas. El gobierno y los sitios universitarios también proveen información muy técnica sobre nuevas tecnologías. En muchos sitios la información que se proporciona entra en diferencia con personas por el poco valor práctico.

Hoy en día los de cracker`s utilizan las mismas herramientas que disponen las organizaciones para la seguridad de la red. Los crackers usan máquinas en las qué sus herramientas son mucho mas poderosas, por lo tanto permiten mayor rapidez y eficiencia al momento de violar la seguridad de las organizaciones. Los crackers se han organizado, y mantienen una amplia variedad de servidores en el Internet. Éstos son establecidos típicamente usando sistemas operativos tales como: Linux o FreeBSD. Los otros son más desconfiables y pueden aparecer en diferentes horas por medio de direcciones dinámicas IP. La mayoría de sitios de cracking y hacking fueron puestos en marcha en plataformas UNIX e IBM. Hay una ausencia sensible de la información de la calidad para los usuarios de Macintosh.

Muchos sitios son legítimas paradas para los cracker`s porque proveen información libremente para la comunidad del Internet. En uno u otro caso, ambos hackers y crackre`s crean sitios Web con excelente información sobre las tecnologías de seguridad.

Así pues, se trafica la información. No hay solución a este problema, y no debe haber. Sería injusto parar la educación de muchos individuos serios, responsables de sus actos. La información tan avanzada y las herramientas de la seguridad seguirán siendo disponibles.

d. La naturaleza humana

Hemos logrado la fuerza final y probablemente la más influyente en el trabajo, para debilitar la seguridad de la organización: La naturaleza humana. Los humanos son, por naturaleza, una raza perezosa. Para la mayoría de usuarios, el tema de seguridad es aburrido y tedioso. Asumen que la seguridad es para personas expertas.

Existen dos aspectos finales en la naturaleza humana que influyen en la evolución de la seguridad. El miedo es uno. La mayoría de compañías tienen miedo para comunicarse con terceros cuando tienen problemas en la seguridad. Por ejemplo, la mayoría de compañías no le dirían a cualquier persona que se ha practicado una abertura en su seguridad. Cuando un sitio Web es agrietado, es noticia extraordinaria; Esto no puede ser evitado. Cuando un sistema es agujerado de una o de otra forma, la cobertura de la prensa o cualquier exposición usualmente puede ser evitada. Entonces, una compañía simplemente puede seguir adelante, negando cualquier incidente, y asegurando su red de la mejor manera posible. Esto priva a la comunidad de datos y estadísticas muy necesitados.

El otro factor humano es la curiosidad. La curiosidad es: una faceta de las experiencias humanas para satisfacer el descubrimiento. La investigación y el descubrimiento son las cosas más importantes en la vida. Aprendemos desde el momento que nacemos hasta el momento que morimos, y a lo largo de ese camino, cada fragmento de la información es útil. Los cracker's no son tan duros de entender. Caen en los fundamentos mas básicos: ¿Por qué esta puerta esta bloqueada? ¿Puedo abrirla? mientras estos aspectos sigan, probablemente el Internet nunca llegue hacer seguro.

2.4.3. ¿Necesita ser el Internet seguro?

Sí. El Internet necesita ser seguro y no simplemente por razones de seguridad nacional. Hoy, es cuestión de seguridad personal. A medida que más instituciones

financieras gravitan por el Internet, el contrato de futuros financieros del mundo dependerá de la seguridad.

Muchos usuarios no pueden ser Conscientes del número de instituciones financieras que ofrecen servios de banca en línea. Unos años atrás, esto Fue un fenómeno relativamente raro.

Los registros bancarios son: sumamente personales y contiene información reveladora. Hasta que el Internet sea seguro, esta información está disponible para cualquier persona con conocimientos o técnicas para crear una puerta de entrada a los sistemas de los bancos en línea. También, el Internet necesita ser segura a fin de que no se degenere en una avenida el espionaje doméstico entre grandes empresas ya que el futuro esta en el comercio electrónico.

El correo electrónico privado es una materia diferente, pero no se deja de lado. Para prevenir a todos los usuarios acerca de la violación a su derecho de la privacidad al menos deberían darse cuenta de los productos disponibles y sus políticas de seguridad, ambos Gratuitamente y con el anuncio publicitario.

Por todas estas razones, el Internet debe volverse seguro.

2.4.4. ¿Puede ser el Internet seguro?

Sí. El Internet puede ser seguro. Pero realizado algunos cambios de manera ordenada, inclusive debe hacerse un aumento de la conciencia pública por el problema.

La mayoría de usuarios Todavía consideran el Internet como un juguete, un dispositivo de entretenimiento que es bueno para un par de horas en una tarde de domingo. Eso necesita cambiar en los años venideros.

El Internet es probablemente, el avance más importante del siglo. Dentro de unos cuantos años, será una fuerza poderosa en la vida de la mayoría de personas. De modo que esta fuerza pueda mantener a las personas informadas correctamente.

Los miembros de los medios noticiosos ciertamente han ayudado a la situación, sin embargo la cobertura del soporte lógico informático del Internet no es siempre precisa. Se ha visto la subida de columnas de tecnología en periódicos a lo largo del mundo para llevar la información a importantes lectores. Sin embargo no es suficiente y se sospecha que el futuro de los periódicos es que desarrollen sus secciones para las noticias del Internet, parecidas a las secciones de interés comun como lo son: las noticias deportivas, noticias locales, noticias medicas etc. Igualmente, muchos usuarios son conscientes, y ese número crece cada día.

2.5. ¿EXISTEN ASPECTOS PRIMORDIALES EN LA SEGURIDAD?

Para mantener un sistema y una red segura o fiable básicamente existen tres aspectos importantes: la confidencialidad, la integridad y la disponibilidad.

¿Que implica cada uno de los tres aspectos que acabamos de mencionar?: La confidencialidad nos dice que los objetos de un sistema han de ser accedidos únicamente por personas autorizadas a ellos, y que esas personas autorizadas no van a convertir esa información en disponible para otras entidades; la integridad significa que los objetos solo pueden ser modificados por personas autorizadas, y de una manera controlada, y la disponibilidad indica que los objetos del sistema tienen que permanecer accesibles a personas autorizadas; es el contrario de la negación de servicio. Generalmente tienen que existir los tres aspectos descritos para que haya seguridad.

Nota: un sistema Linux puede conseguir confidencialidad para un determinado archivo haciendo que ningún usuario ni siquiera el root pueda leerlo, pero este mecanismo no proporciona disponibilidad alguna.

Dependiendo del entorno en que un sistema informático trabaje, a sus responsables les interesara dar prioridad a ciertos aspectos de la seguridad. Por ejemplo, en un sistema militar se antepondrá la confidencialidad de los datos almacenados o transmitidos sobre su disponibilidad. Seguramente, es preferible que alguien borre información confidencial que se podría recuperar después desde una cinta de backup a que ese mismo atacante pueda leerla. En cambio, en un servidor NFS de un departamento, se premiara la disponibilidad frente a la confidencialidad. Importa poco que un atacante lea una unidad, pero que esa misma unidad no sea leída por usuarios autorizados se perderá tiempo y dinero. En un entorno bancario, la faceta que mas preocupa a los responsables del sistema es la integridad de los datos, frente a su disponibilidad o su confidencialidad, es menos grave que un usuario consiga leer el saldo de otro que el hecho de que ese usuario pueda modificarlo.

2.6. ¿QUE NECESITAMOS PROTEGER?

Los tres elementos principales a proteger en cualquier sistema informático son: el software, el hardware y los datos. Por hardware entendemos: el conjunto formado por todos los elementos físicos de un sistema informático, como CPUs, terminales, cableado, medios de almacenamiento primarios y secundarios o tarjetas de red. Por software entendemos: el conjunto de programas lógicos que hacen funcional al hardware, tanto sistemas operativos como aplicaciones, y por datos: el conjunto de información lógica que manejan el software y el hardware, como por ejemplo: paquetes que circulan por un cable de red o entradas de una base de datos. Aunque generalmente en las auditorıas de seguridad se habla de un cuarto elemento a proteger: los fungibles que son: elementos que se gastan o desgastan con el uso continuo, como papel de impresora, toners, cintas magnéticas, diskettes, en nuestra tesis no consideraremos la seguridad de estos elementos.

Habitualmente los datos es el principal elemento de los tres a proteger, ya que es el mas amenazado y seguramente el mas difícil de recuperar. Con toda seguridad una maquina ubicada en un lugar de acceso físico restringido, o al menos controlado, y además en caso de perdida de una aplicación se pueda restaurar sin problemas

desde su medio original por ejemplo, el CD-ROM. Sin embargo, en caso de perdida de una base de datos o de un proyecto de un usuario, no tenemos un medio original para restaurar los datos perdidos.

Contra cualquiera de los tres elementos descritos anteriormente pero principalmente sobre los datos se pueden realizar multitud de ataques o, dicho de otra forma, están expuestos a diferentes amenazas. Generalmente, la estructura elemental de estas amenazas se divide en cuatro grandes grupos: interrupción, interceptación, modificación y fabricación.

Un ataque se clasifica como una interrupción si hace que un objeto del sistema se pierda, quede inútil o no disponible. Se tratara de una interceptación si una persona no autorizado consigue un acceso a un determinado objeto del sistema, y de una modificación si además de conseguir el acceso consigue modificar el objeto; algunos autores consideran un caso especial de la modificación. La destrucción, entendiéndola como una modificación que deja inútil al objeto afectado. Por ultimo, se dice que una a fabricación se trata de una modificación destinada a conseguir un objeto similar al atacado de forma que sea difícil distinguir entre el objeto original y el fabricado.

2.7. ¿DE QUE NOS QUEREMOS PROTEGER?

Nuestros sistemas pueden verse perjudicado por: los humanos, programas y las catástrofes naturales. A continuación se presentan una relación de los elementos que potencialmente pueden amenazar nuestro sistema.

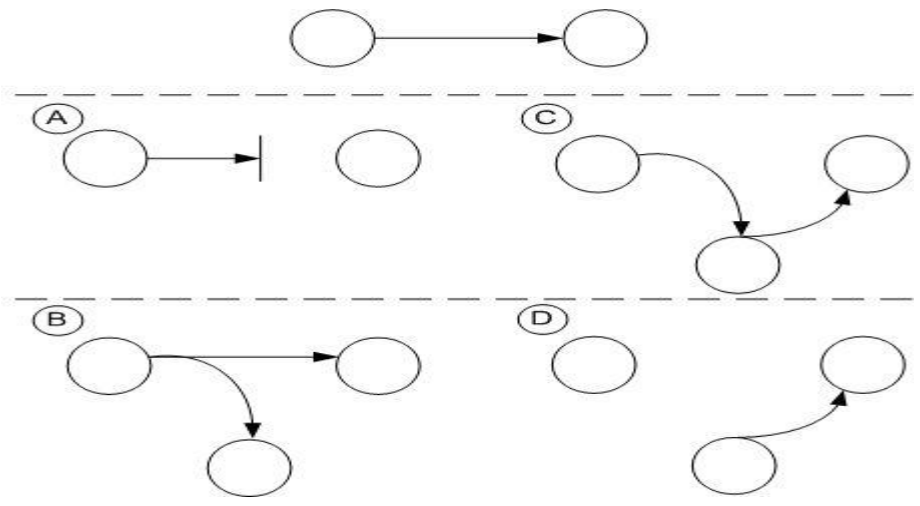


Figura 2.2 Flujo normal de información entre emisor y receptor y posibles amenazas: (a) interrupción, (b) interceptación, (c) modificación y (d) fabricación.

2.7.1 Personas.

La mayoría de ataques a nuestros sistemas va a provenir de personas que, intencionadas, pueden causarnos enormes pérdidas. Generalmente se trata de piratas que intentan conseguir el nivel máximo de privilegio para aprovechar algunos riesgos lógicos especialmente agujeros en el software.

Aquí se describen brevemente los diferentes tipos de personas que de una u otra forma pueden constituir un riesgo para nuestros sistemas; generalmente se dividen en dos grandes grupos: los hacker's y cracker's.

a. Personal.

Las amenazas a la seguridad de un sistema o a la red, provenientes del personal de la propia organización rara vez son tomadas en cuenta, se supone un entorno de confianza donde a veces no existe, por lo que se pasa por alto el hecho de que casi cualquier persona de la organización, incluso el personal ajeno a la infraestructura informática como lo es: la secretaria, el personal de seguridad, personal de limpieza y mantenimiento puede comprometer la seguridad de los equipos. Aunque los ataques pueden ser intencionados, lo normal es que los ataques se traten como

accidentes causados por un error o por desconocimiento de las normas básicas de seguridad.

b. Ex-empleados.

Otro gran grupo de personas potencialmente interesadas en atacar nuestro sistema son los antiguos empleados, especialmente los que no abandonaron el entorno por voluntad propia. Generalmente, se trata de personas descontentas con la organización que pueden aprovechar debilidades de un sistema que conocen perfectamente para dañarlo como venganza por consideran algún hecho injusto: amparados en excusas como 'No me han pagado lo que me deben' o 'no me han puesto donde quiero estar' puede ser la causa para insertar troyanos, bombas lógicas, virus o simplemente conectarse al sistema como si aun trabajaran para la organización porque muchas veces se mantienen las cuentas abiertas incluso meses después de abandonar la empresa.

c. Curiosos.

Los curiosos son los atacantes más habituales en los sistemas. Recordemos que las instituciones están trabajando para formar a futuros profesionales de la informática. Además recordemos también que las personas suelen ser curiosas por naturaleza. Esta combinación produce una avalancha de estudiantes o personal intentando conseguir mayor privilegio del que tienen o intentando acceder a sistemas a los que oficialmente no tienen acceso. En la mayoría de ocasiones esto se hace simplemente para leer el correo de un amigo, enterarse de cuanto cobra un compañero de trabajo, copiar un trabajo o comprobar que es posible romper la seguridad de un sistema en concreto. Aunque en la mayoría de situaciones se trata de ataques no destructivos, esto no beneficia en absoluto al entorno de fiabilidad que podamos generar en un determinado sistema.

d. Crackers

Los entornos de seguridad media son un objetivo típico de los crackers, ya sea para fisgonear, destruir, para utilizarlas como enlace hacia otras redes o simplemente por diversión. Por otro lado, son redes generalmente abiertas, con un gran número y

variedad de sistemas conectados a estas redes que provoca, casi por simple probabilidad, que al menos algunos de sus equipos sean vulnerables a problemas. De esta forma un atacante solo utiliza un escaner de seguridad contra el dominio completo y luego atacar mediante un simple exploit para ver las vulnerabilidades de los sistemas. Esto convierte a las redes, empresas y los ISP en un objetivo fácil y apetecible para piratas con cualquier nivel de conocimientos, desde los más novatos hasta los expertos, que pueden utilizar toda la red para probar nuevos ataques o como nodo intermedio en un ataque a otros organismos.

e. Cracker's remunerados.

Este es el grupo de atacantes mas peligroso de un sistema, este tipo de personas suele afectar a las grandes empresas o a organismos de defensa. Se trata de piratas con gran experiencia en problemas de seguridad y un amplio conocimiento de sistemas, estos son pagados por terceros para robar secretos como por ejemplo: el nuevo diseño de un procesador, una base de datos de clientes, información confidencial sobre las posiciones de satélites espías o simplemente para dañar la imagen de la entidad afectada.

Estos terceros suele ser: una empresa de la competencia o un organismo de inteligencia, es decir, una organización que puede permitirse un gran gasto en el ataque; de ahí su peligrosidad. Se suele pagar bien a los mejores piratas, y por si esto fuera poco los atacantes van a tener todos los medios necesarios a su alcance. Aunque estos intrusos remunerados son los menos comunes en la mayoría de situaciones.

f. Terroristas

Por terroristas no debemos entender simplemente a los que se dedican a poner bombas o quemar autobuses; bajo esta definición se engloba a cualquier persona que ataca al sistema simplemente por causar algún tipo de daño. Por ejemplo, alguien puede intentar borrar las bases de datos de un partido político enemigo o destruir los sistemas de archivos de un servidor que alberga páginas Web de algún

grupo religioso. En el caso de redes I+D, son típicos los ataques en los sistemas o en la modificación de paginas Web de algún departamento.

2.7.2. Amenazas lógicas.

Bajo la etiqueta de amenazas lógicas encontramos todo tipo de programas que han sido creados de forma intencionada o simplemente por error para dañar nuestra red o sistema. Entre las amenazas lógicas están:

a. Software incorrecto.

Las amenazas mas habituales a un sistema provienen de errores cometidos de forma involuntaria por los programadores de sistemas o de aplicaciones. Una situación no contemplada a la hora de diseñar una aplicación o un error accediendo a memoria pueden comprometer local o remotamente a cualquier sistema operativo.

A estos errores de programación se les denomina bugs, y a los programas utilizados para aprovechar uno de estos fallos y atacar al sistema se les denomina exploits. Los exploits representan la amenaza mas común contra cualquier sistema, ya que cualquiera puede conseguirlo para utilizarlo en nuestra contra sin tener el mínimo conocimiento del sistema operativo; incluso hay exploits que dañan seriamente la integridad de un sistema y estos están preparados para ser utilizados desde MS-DOS, con lo que cualquier pirata novato comúnmente denomina Script Kiddies puede utilizarlos contra un servidor y conseguir un control total de una maquina de varios millones de dólares desde su PC sin saber nada del sistema atacado.

b. Herramientas de seguridad.

Cualquier herramienta de seguridad representa un arma de doble filo: de la misma forma que un administrador las utiliza para detectar y solucionar fallos en sus sistemas o en la subred completa, un potencial intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos. Herramientas como nessus, saint o Satán pasan de ser útiles a ser peligrosas cuando las utilizan crackers que buscan información sobre las vulnerabilidades de un host o de una red completa.

La conveniencia de diseñar y distribuir libremente herramientas que puedan facilitar un ataque es un tema delicado; incluso expertos reconocidos como Alec Muffet autor del adivinador de contraseñas Crack han recibido enormes críticas por diseñar determinadas herramientas de seguridad para Unix.

Tras numerosos debates sobre el tema, ha quedado bastante claro que no se puede basar la seguridad de un sistema en el supuesto desconocimiento de sus problemas. Por parte de los atacantes: esta política, denominada la seguridad a través de la oscuridad (Security through obscurity), se ha demostrado inservible en múltiples ocasiones. Si como administradores no utilizamos herramientas de seguridad que muestren las debilidades de nuestros sistemas para corregirlas, tenemos que estar seguro que un atacante no va a dudar en utilizar tales herramientas para explotar las debilidades encontradas en los sistemas.

c. Puertas traseras.

Durante el desarrollo de aplicaciones grandes o de sistemas operativos es habitual entre los programadores insertar atajos en los sistemas de autenticación del programa o del núcleo que se esta diseñando. A estos atajos se les denomina puertas traseras, y con ellos se consigue mayor velocidad a la hora de detectar y depurar fallos: por ejemplo, los diseñadores de un software de gestión de bases de datos en el que para acceder a una tabla se necesitan cuatro claves diferentes de diez caracteres cada una pueden insertar una rutina para conseguir ese acceso mediante una clave especial, con el objetivo de perder menos tiempo al depurar el sistema.

Algunos programadores pueden dejar estos atajos en las versiones definitivas de su software para facilitar un mantenimiento posterior, para garantizar su propio acceso, o simplemente por descuido; la cuestión es que si un atacante descubre una de estas puertas traseras va a tener un acceso global a datos, lo que es un grave peligro para la integridad de nuestro sistema.

d. Bombas lógicas.

Las bombas lógicas son partes de código de ciertos programas que permanecen sin realizar ninguna función hasta que son activadas. En ese punto, la función que realizan no es la original del programa, sino que generalmente se trata de una acción perjudicial. Los activadores más comunes de estas bombas lógicas pueden ser la ausencia o presencia de ciertos archivos o la llegada de una fecha concreta. Si las activa el root, el administrador o el programa que contiene la bomba, los efectos pueden ser fatales.

e. Canales cubiertos.

La definición de los canales cubiertos o canales ocultos, según otros autores son: canales de comunicación que permiten a un proceso transferir información de forma que viole la política de seguridad del sistema; dicho de otra forma, un proceso transmite información a otras personas ya sean locales o remotos que no estén autorizados a leer dicha información.

Los canales cubiertos no son una amenaza demasiado habitual en redes de I+D, ya que suele ser mucho mas fácil para un atacante aprovechar cualquier otro mecanismo de ataque lógico. Sin embargo, es posible su existencia, y en este caso su detección suele ser difícil, algo tan simple como el puerto finger abierto en una maquina puede ser utilizado a modo de covert channel por un pirata con algo de experiencia.

f. Virus.

Un virus es una secuencia de código que se inserta o se aloja en un archivo ejecutable denominado huésped, de forma que cuando el archivo se ejecuta, el virus también lo hace, insertándose a sı mismo en otros programas.

Todo el mundo conoce los efectos de los virus en algunos sistemas operativos. Sin embargo, en Linux los virus no suelen ser un problema de seguridad grave, Los virus existentes para entornos Unix son mas una curiosidad que una amenaza real. Ciertos virus, especialmente los de boot, pueden tener efectos nocivos, como dañar

el sector de arranque; aunque se trata de daños menores comparados con los efectos de otras amenazas.

g. Gusanos.

Un gusano es un programa capaz de ejecutarse y propagarse por sı mismo a través de redes, en ocasiones portando virus o aprovechando los bugs en los sistemas para dañarlos.

Al ser difíciles de programar su número no es muy elevado, pero el daño que pueden causar es muy grande: El mayor incidente de seguridad en el Internet fue precisamente: el Internet Worm, un gusano que en 1988 causo pérdidas millonarias al infectar y detener mas de 6000 maquinas conectadas a la red.

Un gusano puede automatizar y ejecutar en unos segundos todos los pasos que seguiría un atacante humano para acceder a nuestro sistema, mientras que una persona, por muchos conocimientos y medios que posea, tardaría como mínimo horas en controlar nuestra red completa, un gusano puede hacer eso mismo en pocos minutos: de ahí su enorme peligro y sus devastadores efectos.

h. Caballos de Troya.

Los troyanos o caballos de Troya son instrucciones escondidas en un programa de forma que este realiza las tareas que el usuario espera de el, pero realmente ejecuta funciones ocultas sin el conocimiento del usuario. Como el Caballo de Troya de la mitología griega, al que deben su nombre, ocultan su función real bajo la apariencia de un programa inofensivo que a primera vista funciona correctamente.

En la práctica los ataques a Unix, cuando un intruso consigue el privilegio necesario en el sistema instala troyanos para ocultar su presencia o para asegurarse la entrada en caso de ser descubierto. Por ejemplo, es típico utilizar lo que se denomina un rootkit, que no es mas que un conjunto de versiones troyanas de ciertas utilidades como son: netstat, ps, who, para conseguir que cuando el administrador las ejecute no vea la información relativa al atacante, como sus procesos o su conexión al sistema; otro programa que se suele suplantar es login, por ejemplo para que al

recibir un cierto nombre de usuario y contraseña proporcione acceso al sistema sin necesidad de consultar /etc/passwd

.

i. Programas conejo o bacterias

Bajo este nombre se conoce a los programas que no hacen nada útil, sino que simplemente se dedican a reproducirse hasta que el número de copias acaba con los recursos del sistema por ejemplo: memoria, procesador, disco. Produciendo una negación de servicio. Por sı mismos no hacen ningún daño, sino que lo que realmente perjudica es el gran numero de copias suyas en el sistema, que en algunas situaciones pueden llegar a provocar la parada total de una maquina.

Hay ciertos programas que pueden actuar como conejos sin proponérselo por ejemplos es muy común que un bucle que por error se convierte en infinito y que contenga entre sus instrucciones algunas reservas de memoria, lo que implica que si el sistema no presenta una correcta política de cuotas para procesos de usuario pueda venirse abajo o degradar enormemente sus prestaciones.

j. Técnicas salami.

Por técnica salami se conoce al robo automatizado de pequeñas cantidades de bienes donde generalmente es dinero en una gran cantidad. El hecho de que la cantidad inicial sea grande y la robada pequeña hace extremadamente difícil su detección: si de una cuenta con varios millones de dólares se roban unos centavos , nadie va a darse cuenta de ello; si esto se automatiza para, por ejemplo, descontar una centavo de cada nomina pagada en la universidad o de cada beca concedida, tras un mes de actividad seguramente se habrá robado una enorme cantidad de dinero sin que nadie se haya percatado de este hecho, ya que de cada origen se ha tomado una cantidad insignificante.

Las técnicas salami no se suelen utilizar para atacar sistemas normales, sino que su uso mas habitual es en sistemas bancarios; sin embargo, como en una red con requerimientos de seguridad es posible que haya ordenadores dedicados a

contabilidad, facturación de un departamento o gestión de nominas del personal es muy probable que la amenaza se disminuya.

2.7.3. Modos comunes de ataque

Los tres tipos mas comunes de ataques que los hackers implementan son: IP spoofing, sniffing y negación de servicios (Denial of Services – DoS).

a. IP Spoofing

IP spoofing es usado para engañar al servidor objetivo acerca del origen de los paquetes TCP/IP. Para el servidor, le parece que los paquetes de datos se han originado desde una dirección IP autentica. Actualmente, estos paquetes son enviados desde un cliente que esta usando una dirección IP que no es propia. El cracker normalmente utiliza una dirección IP en la cual el servidor confía pero es una dirección falsa. Por lo tanto, el cracker se aprovecha de la confianza entre el sistema objetivo y el sistema atacado.

Para entender el ataque de IP spoofing hay que considerar el siguiente escenario:

- Dirección IP del servidor: 201.13.12.1
- Dirección IP del cliente verdadera: 201.45.12.2
- Dirección IP del cliente falsa: 180.74.5.2

En este escenario, el servidor objetivo con la dirección IP 201.13.12.1 es guiado a creer que los paquetes de datos vienen desde el cliente con la dirección 180.74.5.2, donde el emisor actual de los paquetes es el cliente con la dirección IP 201.45.12.2. el servidor, en este caso confía en la dirección falsa.

b. Sniffing

Sniffing es el proceso de capturar paquetes de red para interceptar la comunicación de la cual es sniffer no forma parte. El proceso de sniffing involucra el uso de

software que normalmente es usado para monitorear y en el diagnostico de la red, al igual que el monitor de red.

El sniffing es realizado al poner una tarjeta de red de forma que pueda escuchar todos los mensajes de broadcast en un segmento particular de red en el cual reside. Los paquetes de red son analizados para obtener información confidencial como nombres de usuarios y passwords. Los passwords obtenidos de esta manera pueden ser utilizados después para propósitos destructivos.

c. Ataque de negación de servicios – DoS

Los ataques DoS involucra la incapacidad del servidor objetivo o red de servir a clientes legítimos. Los atacantes inundan el sistema objetivo con paquetes y consumen el espacio de memoria disponible. Dando como resultado, el sistema objetivo es incapaz de servir a clientes legítimos por un cierto periodo de tiempo o hasta que la recuperación sea efectuada.

Los ataques de DoS pueden ser ataques de fuerza bruta, en los cuales el atacante intenta obstruir todos los recursos del sistema objetivo o estos pueden atacar ciertas vulnerabilidades en el protocolo TCP/IP y implementaciones pv4.

A continuación de muestran los ataques DoS que los hackers emplean mas comúnmente:

d. Ping de la muerte

El ataque del ping de la muerte solía ser una forma de ataque popular, pero la mayoría de sistemas hoy en día tienen seguridad en contra de esta vulnerabilidad. Este ataque involucra el hacer ping al sistema objetivo con un paquete de datos que es mas largo que el numero máximo de bytes permitidos por TCP/IP. Esto causa normalmente causa que el sistema objetivo pare de responder o reinicie.

e. Ataque de la lágrima

El ataque de la lágrima involucra el uso de campos de superposición de offset en las cabeceras TCP de los paquetes de datos. Este paquete busca desestabilizar el sistema objetivo cuando este trata de reensamblar los paquetes de datos, lo cual causa que el sistema objetivo pare de responder o reinicie.

f. Ataque SYN

El ataque SYN es una forma de ataque spoofing. El atacante envía un numero de peticiones de sincronización hacia el sistema objetivo con una dirección IP origen falsa. El sistema objetivo responde con un paquete SYN/ACK y espera por el paquete ACK desde el cliente no existente. Como resultado, la petición es almacenada en cola, lo cual a largo plazo reduce los recursos del sistema objetivo.

g. Ataques DoS distribuidos

Los ataques DoS distribuidos utilizan redes más pequeñas y menos protegidas como plataforma de ataque hacia redes más seguras. Los hackers primero atacan y toman el control de redes más pequeñas y posteriormente utilizan estas redes para lanzar ataques DoS en contra de una red objetivo superior. Al seguir esta estrategia, el hacker hace más difícil al administrador de red en la red objetivo el rastreo del hacker porque este puede manipular los registros (logs) de las redes intermedias las cuales son menos seguras.

2.7.4. Catástrofes.

Las catástrofes naturales son las amenazas menos probables contra los entornos habituales. Simplemente por su ubicación geográfica, a nadie se le escapa que la probabilidad de sufrir un terremoto o una inundación que afecte a los sistemas informáticos en una gran ciudad como Madrid, Viena, Asunción, entre otros es relativamente baja, al menos en comparación con el riesgo de sufrir un intento de acceso por parte de un pirata o una infección por virus. Sin embargo, el hecho de que las catástrofes sean amenazas poco probables no implica que contra ellas no se tomen medidas básicas, ya que si se produjeran generarían enormes daños.

Un subgrupo de las catástrofes es el denominado riesgo poco probable. Obviamente se denomina así al conjunto de riesgos que, aunque existen, la posibilidad de que se produzcan es tan baja, que nadie toma, o nadie puede tomar, medidas contra ellos. Ejemplos habituales de riesgos poco probables son: un ataque nuclear contra el sistema, el impacto de un satélite contra la sala de operaciones, o el secuestro de un operador por una nave extraterrestre. Nada nos asegura que este tipo de catástrofes no vaya a ocurrir, pero la probabilidad es tan baja y los sistemas de prevención tan costosos que no vale la pena tomar medidas contra ellas. Como ejemplos de catástrofes hablaremos de terremotos, inundaciones, incendios, humo o atentados de baja magnitud. Los riesgos poco probables los trataremos sin profundizar.

2.8. ¿CÓMO NOS PODEMOS PROTEGER?

Para proteger nuestro sistema tenemos que realizar un análisis de las amenazas potenciales que puede sufrir, las perdidas que podrían generar, y la probabilidad de su ocurrencia; a partir de este análisis se tiene que diseñar una política de seguridad que defina responsabilidades y reglas a seguir para evitar tales amenazas o minimizar sus efectos en caso de que se produzcan.

Hasta ahora hemos hablado de los aspectos que engloba la seguridad informática, de los elementos a proteger, de los tipos de amenazas que se presentan y del origen de tales amenazas. Para completar nuestra visión en seguridad, necesitamos hablar de las formas de protección de los sistemas.

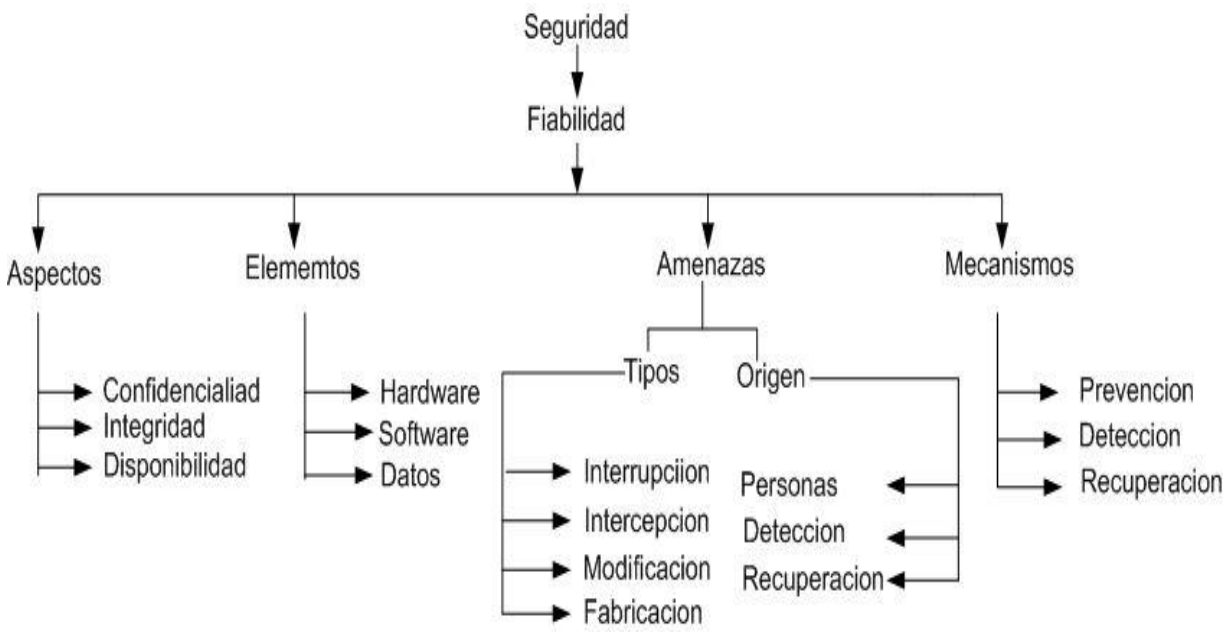


Figura 2.3 Visión global de la seguridad informática

Los mecanismos utilizados para implementar esta política de seguridad se les denomina mecanismos de seguridad; estos son la parte más visible de nuestro sistema de seguridad, convirtiéndose en las herramientas básicas para garantizar la protección de los sistemas o de la propia red.

Los mecanismos de seguridad se dividen en tres grandes grupos: de prevención, de detección y de recuperación. Los mecanismos de prevención son aquellos que aumentan la seguridad de un sistema durante el funcionamiento normal, previniendo la ocurrencia de violaciones a la seguridad; por ejemplo, el uso de cifrado en la transmisión de datos se puede considerar como un mecanismo de este tipo, ya que evita que un posible atacante escuche las conexiones hacia o desde un sistema operativo en la red. Por mecanismos de detección se conoce a aquellos que se utilizan para detectar violaciones en seguridad o intentos de violación; ejemplos de estos mecanismos son los programas de auditoria como Tripwire. Finalmente, los mecanismos de recuperación son aquellos que se aplican cuando una violación del sistema se ha detectado, para retornar a este a su funcionamiento correcto; ejemplos de estos mecanismos son la utilización de copias de seguridad o el hardware adicional. Dentro de este ultimo grupo de mecanismos de seguridad encontramos un

subgrupo denominado mecanismos de análisis forense, cuyo objetivo no es simplemente retornar al sistema a su modo de trabajo normal, sino averiguar el alcance de la violación, las actividades de un intruso en el sistema, y la puerta utilizada para entrar; de esta forma se previenen ataques posteriores y se detectan ataques a otros sistemas de nuestra red.

Aunque los tres tipos de mecanismos son importantes para la seguridad de nuestra red o sistema. Se tiene que enfatizar en el uso de mecanismos de prevención y de detección; el máximo dicho popular 'mas vale prevenir que curar' se puede aplicar en la seguridad informática: para nosotros, evitar un ataque, detectar un intento de violación, o detectar una violación exitosa inmediatamente después de que ocurra es mucho mas productivo y menos comprometedor para el sistema que restaurar el estado tras una violación a la maquina. Es mas, si consiguiéramos un sistema sin vulnerabilidades y cuya política de seguridad se implementara mediante mecanismos de prevención de una forma completa, no necesitaríamos mecanismos de detección o recuperación. Pero esto seria irreal.

Los mecanismos de prevención más habituales en las redes son los siguientes:

a. Mecanismos de autenticación e identificación.

Estos mecanismos hacen posible identificar entidades del sistema de una forma única, y posteriormente, una vez identificadas, autenticarlas (comprobar que la entidad es quien dice ser). Son los mecanismos más importantes en cualquier sistema, ya que forman la base de otros mecanismos que basan su funcionamiento en la identidad de las entidades que acceden a un objeto.

Un grupo especialmente importante de estos mecanismos son los denominados Sistemas de Autenticación de Usuarios, en nuestro caso es el modelo de seguridad AAA (autorización, autenticación y contabilidad) al que se prestara una especial atención por ser uno de los más utilizados en la práctica.

b. Mecanismos de control de acceso.

Cualquier objeto del sistema debe estar protegido mediante un mecanismo de control de acceso, estos controlan todos los tipos de acceso sobre el objeto por parte de cualquier entidad del sistema. Dentro de linux, el control de acceso más habitual es el discrecional (DAC, Discretionary Access Control), implementado por los bits rwx y las listas de control de acceso para cada objeto del sistema; sin embargo, también se permiten especificar controles de acceso obligatorio por medio de la MAC.

c. Mecanismos de separación.

Cualquier sistema con diferentes niveles de seguridad ha de implementar mecanismos que permitan separar los objetos dentro de cada nivel, evitando el flujo de información entre objetos y entidades de diferentes niveles siempre que no exista una autorización del mecanismo de control de acceso.

Los mecanismos de separación se dividen en cinco grandes grupos, en función de como separan a los objetos: separación física, temporal, lógica, criptográfica y fragmentación. Dentro de Linux, el mecanismo de separación mas habitual es el de separación lógica o aislamiento, implementado en algunos sistemas mediante una Base de Computadoras Confiables (trusted computer Base TCB).

d. Mecanismos de seguridad en las comunicaciones.

Es importante para la seguridad de nuestro sistema el proteger la integridad y la privacidad de los datos cuando se transmiten a través de la red. Para garantizar esta seguridad en las comunicaciones, se tienen que utilizar ciertos mecanismos, la mayoría de los cuales se basan en la criptografía: cifrado de clave pública, de clave privada y firmas digitales.

Una de las mayores amenazas a la integridad de las redes es el trafico sin cifrar, que hace extremadamente fáciles los ataques encaminados a robar contraseñas o suplantar la identidad de maquinas en la red. A lo largo de esta tesis intentaremos explicar el funcionamiento de algunos de estos mecanismos para conseguir que las redes y los sistemas operativos sean más fiables.

CAPITULO 3. POLÍTICAS DE SEGURIDAD DE UNA RED CORPORATIVA

Describe la forma de realizar y de implementar las políticas de seguridad en una corporación. Además proporcionan mecanismos de comunicación entre la gerencia y el usuario de lo que esta permitido o no en la red.

Puntos clave.

- concepto general de política de seguridad de red corporativa.
- parámetros para establecer políticas de seguridad y quien las establece.
- estableciendo políticas estratégicas de la red corporativa.

3.1. PROPOSICIÓN DE UNA FORMA DE REALIZAR EL ANÁLISIS PARA LLEVAR A CABO LA ELABORACIÓN DE LAS POLÍTICAS.

A continuación en la figura 3.1 se presenta un diagrama para poder crear las políticas ya sea para una corporación o cualquier entidad que necesite implementarlas.

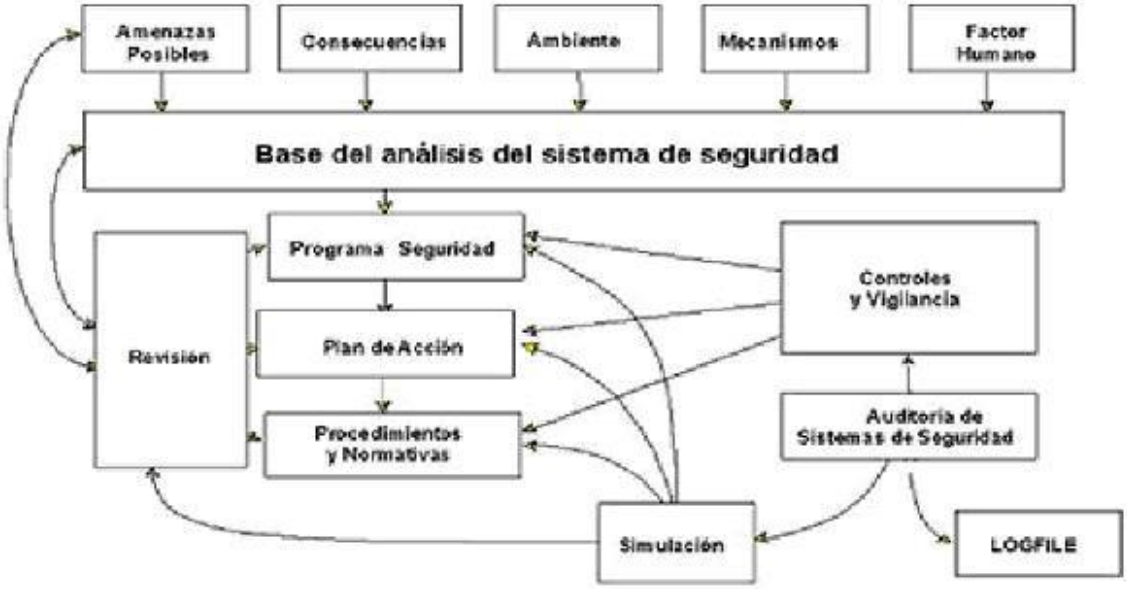


Figura 3.1 Proposición para la elaboración de políticas

En la figura 3.1 están plasmados todos los módulos que intervienen para el estudio de una política de seguridad.

Se comienza realizando una evaluación del factor humano que interviene, teniendo en cuenta que éste es el punto más vulnerable en toda la cadena de seguridad. El medio ambiente juega un papel importante en el desempeño de los sistemas, porque las consecuencias que pueden traer ya sean: pérdidas físicas, pérdidas económicas, o en la imagen de la organización, son muy grandes y por ultimo cuáles son las amenazas posibles. Una vez evaluado todo lo anterior, se origina un programa de seguridad basado en políticas, que involucra los pasos a tomar para poder llegar a tener la seguridad deseada. Luego, se pasa al plan de acción, que es cómo se va a llevar a cabo el programa de seguridad. Finalmente, se redactan los procedimientos y normas que se utilizaran dentro de la organización.

Con el propósito de asegurar el cumplimiento de todo lo anterior, se realizan los controles y la vigilancia que aseguran el fiel cumplimiento de lo propuesto anteriormente. Para asegurar un marco efectivo, se realizan auditorias a los controles y a los archivos logísticos que se generen en los procesos implementados (de nada vale tener archivos logísticos si nunca se analizan o se analizan cuando ya ha ocurrido un problema). Con el objeto de confirmar el buen funcionamiento de lo creado, se procede a simular eventos que atenten contra la seguridad interna y externa del sistema o de la red. Como el proceso de seguridad es un proceso dinámico, es necesario realizar revisiones al programa de las políticas de seguridad, el plan de acción a los procedimientos y las normas.

3.2. VISION GENERAL DE LAS POLÍTICA DE SEGURIDAD.

Las organizaciones deben hacer cumplir políticas obligatorias de seguridad, en la cual puedan implementarse eficientemente las reglas del acceso y el manejo de la información sensitiva. Estas reglas deben de incluir requisitos tales como: Ninguna persona que carezca de los permisos apropiados obtendrá el acceso a la información clasificada. Además, los controles de seguridad discrecional se requieren para asegurar que solamente los usuarios o los grupos seleccionados de usuarios puedan obtener el acceso a los datos.

Debe existir una política de seguridad explícita y bien reforzada por el sistema. Identificando los eventos y los objetos, para crear un conjunto de reglas que son utilizadas por el sistema para determinar si un evento dado puede permitir el acceso a un objeto específico.

En este sentido, las Políticas de Seguridad Informática (PSI), surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos. Estos permiten a la compañía desarrollarse y mantenerse en su sector de negocios.

3.3. ¿QUE SON LAS POLÍTICAS DE SEGURIDAD?

La Seguridad Informática no tiene una solución definitiva aquí y ahora, sino que es y será el resultado de la innovación tecnológica, a la par del avance tecnológico por parte de aquellos que son los responsables de nuestros sistemas.

El término política de seguridad se suele definir como: el conjunto de requisitos definidos por los responsables directos o indirectos de un sistema que indica generalmente qué está y qué no está permitido en el área de seguridad durante la operación general de dicho sistema. Al tratarse de términos generales, aplicables a situaciones o recursos muy diversos, suele ser necesario afinar los requisitos de la política para convertirlos en indicaciones precisas de qué es lo permitido y lo denegado en cierta parte de la operación del sistema, lo que se denomina política de aplicación específica.

La RFC 1244 define Política de Seguridad como: “una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requerirán”.

La política se refleja en una serie de normas, reglamentos y protocolos a seguir, donde se definen las medidas a tomar para proteger la seguridad del sistema; pero, ante todo, una política de seguridad es una forma de comunicarse con los usuarios.

De acuerdo con lo anterior, al proponer o identificar una política de seguridad se requiere:

- Un alto compromiso con la organización
- Agudeza técnica para establecer fallas
- Agudeza técnica para establecer debilidades
- Constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

3.4. ¿EN QUÉ CONSISTEN LAS POLÍTICAS?

Las políticas implementadas deben controlar quién accede a determinadas áreas de la red y cómo impedir que usuarios no autorizados ingresen a zonas restringidas. Por ejemplo, es común que sólo los integrantes del departamento de recursos humanos puedan acceder a los historiales de sueldo de los empleados.

Las contraseñas generalmente impiden que los empleados accedan a zonas restringidas, pero solamente si tales contraseñas se mantienen en confidencialidad. La política escrita de como advertir a los empleados que no dejen por escrito sus contraseñas en áreas de trabajo, pueden prevenir las violaciones a la seguridad. Los clientes o proveedores con acceso a determinadas partes de la red también deben regirse por las políticas de reglamentación.

Una política de seguridad puede ser prohibitiva, si todo lo que no está expresamente permitido está denegado, o permisiva, si todo lo que no está expresamente prohibido está permitido. La primera aproximación es mucho mejor que la segunda de cara a mantener la seguridad; en este caso la política contemplaría todas las actividades que se pueden realizar en los sistemas, y el resto serían consideradas ilegales.

3.5. ¿QUIÉN IMPLEMENTARÁ Y ADMINISTRARÁ LAS POLÍTICAS?

Los individuos o grupos de personas que custodian y mantienen la red y la seguridad de la misma deben tener acceso a todas las áreas de la red. Por lo tanto, la función de administración de la política de seguridad debe asignarse a personas de confianza y con el conocimiento técnico necesario. Tal como se mencionó anteriormente, la mayoría de las violaciones a la seguridad se realizan desde una red publica o desde el interior de la corporación, por lo tanto este individuo o equipo no debe ser una amenaza en potencia.

Una vez asignados, los administradores de red deben aprovechar las herramientas de software sofisticado que pueden servir para definir, distribuir, implementar y auditar las políticas de seguridad a través de interfaces basadas en explorador.

3.6. ELEMENTOS DE UNA POLÍTICA DE SEGURIDAD INFORMÁTICA.

Una política de seguridad informática (PSI) debe orientar las decisiones que se toman en relación con la seguridad. Por lo tanto, se requiere de una disposición por parte de cada uno de los miembros de la empresa para lograr una visión conjunta de lo que se considera importante.

Las PSI deben considerar los siguientes elementos:

Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.

- Disponibilidad para garantizar que los recursos del sistema se encontrarán disponibles cuando se necesitan, especialmente la información crítica.
- La utilidad de los recursos del sistema y de la información manejada en el mismo.
- Es una invitación de la organización a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Invitación que debe concluir en una posición.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición
- Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización
- Requerimientos mínimos para configuración de la seguridad de los sistemas que cobija el alcance de la política.
- Definición de violaciones y de las consecuencias del no cumplimiento de la política.

- Responsabilidades de los usuarios con respecto a la información a la que ella tiene acceso.
- La integridad de la información del sistema debe estar disponible tal y como se almacenó por un agente autorizado.
- La autenticidad del sistema ha de ser capaz de verificar la identidad de sus usuarios, y los usuarios la del sistema.
- La confidencialidad de La información sólo ha de estar disponible para agentes autorizados, especialmente su propietario.
- Los propietarios de un sistema deben de ser capaces de controlarlo en todo momento; perder este control en favor de un usuario malicioso compromete la seguridad del sistema hacia el resto de usuarios.

3.7. ALGUNOS PARÁMETROS PARA ESTABLECER POLÍTICAS DE SEGURIDAD.

Si bien las características de las PSI que hemos mencionado hasta el momento, nos muestran una perspectiva de las implicaciones en la formulación de estas directrices, revisaremos a continuación, algunos aspectos generales recomendados para la formulación de las mismas.

- Considere efectuar un ejercicio de análisis de riesgos informático, a través del cual valore sus activos, el cual le permitirá afinar las PSI de su organización.
- Involucre a las áreas propietarias de los recursos o servicios, pues ellos poseen la experiencia y son fuente principal para establecer el alcance y las definiciones de violaciones a las PSI.
- Comunique a todo el personal involucrado en el desarrollo de las PSI, los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.

- Recuerde que es necesario identificar quién tiene la autoridad para tomar decisiones, pues son ellos los responsables de salvaguardar los activos críticos de la funcionalidad de su área u organización.
- Desarrolle un proceso de monitoreo periódico de las directrices en el hacer de la organización, que permita una actualización oportuna de las mismas.
- No dé por hecho algo que es obvio. Haga explícito y concreto los alcances y propuestas de seguridad, con el propósito de evitar sorpresas y malos entendidos en el momento de establecer los mecanismos de seguridad que respondan a las PSI trazadas.
- Las PSI deben ofrecer explicaciones comprensibles acerca de por qué deben tomarse ciertas decisiones, transmitir por qué son importantes estos u otros recursos o servicios.
- Las PSI establecen las expectativas de la organización en relación con la seguridad y lo que ella puede esperar de las acciones que la materializan en la compañía. Deben mantener un lenguaje común libre de tecnicismos y términos legales que impidan una comprensión clara de las mismas, sin sacrificar su precisión y formalidad dentro de la empresa.
- La política debe especificar la autoridad que debe hacer que las cosas ocurran, el rango de los correctivos y sus actuaciones que permitan dar indicaciones sobre la clase de sanciones que se puedan imponer. No debe especificar con exactitud qué pasara o cuándo algo sucederá; no es una sentencia obligatoria de la ley.
- Las PSI como documentos dinámicos de la organización, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la planta de personal, cambio en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, cambio o diversificación de negocios entre otros.

3.8. ¿POR QUÉ LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA GENERALMENTE NO CONSIGUEN IMPLANTARSE?

Muchas veces, las organizaciones realizan grandes esfuerzos para definir sus directrices de seguridad y concretarlas en documentos que orienten las acciones de las mismas, con relativo éxito. Hoy en día resulta una labor ardua convencer a los altos ejecutivos de la necesidad de buenas políticas y prácticas de seguridad informática.

Muchos de los inconvenientes se inician por los tecnicismos informáticos y por la falta de una estrategia de mercadeo de los especialistas en seguridad que, llevan a los altos directivos a pensamientos como: "más dinero". Esta situación ha llevado a que muchas empresas con activos muy importantes, se encuentren expuestas a graves problemas de seguridad que, en muchos de los casos, lleva a comprometer su información sensible y por ende su imagen corporativa. Ante esta encrucijada, los encargados de la seguridad deben asegurarse de que las personas relevantes entiendan los asuntos importantes de la seguridad, conocen sus alcances y están de acuerdo con las decisiones tomadas en relación con esos asuntos.

En particular, la gente debe conocer las consecuencias de sus decisiones, incluyendo lo mejor y lo peor que podría ocurrir. Un intrusión o una travesura puede convertir a las personas que no entendieron, en blanco de las políticas o en señuelos de los verdaderos vándalos. Luego, para que las PSI logren abrirse espacio en el interior de una organización deben integrarse a las estrategias del negocio, a su misión y visión, con el propósito de que los que toman las decisiones reconozcan su importancia e incidencias en las proyecciones y utilidades de la compañía.

De igual forma, las PSI deben ir acompañadas de una visión de negocio que promueva actividades que involucren a las personas en su hacer diario, donde se identifiquen las necesidades y acciones que materializan las políticas. En este contexto, entender la organización, sus elementos culturales y comportamientos nos debe llevar a reconocer las pautas de seguridad necesarias y suficientes que

aseguren confiabilidad en las operaciones y funcionalidad de la compañía. A continuación, mencionamos algunas recomendaciones para concientizar sobre la seguridad informática:

- Desarrolle ejemplos organizacionales relacionados con fallas de seguridad que capten la atención de sus interlocutores.
- Asocie el punto anterior a las estrategias de la organización y a la imagen que se tiene de la organización en el desarrollo de sus actividades.
- Articule las estrategias de seguridad informática con el proceso de toma de decisiones y los principios de integridad, confidencialidad y disponibilidad de la información. Muestre una valoración costo-beneficio, ante una falla de seguridad.
- Justifique la importancia de la seguridad informática en función de hechos y preguntas concretas, que muestren el impacto, limitaciones y beneficios sobre los activos claves de la organización.

3.9. EL RIESGO.

Al no definir adecuadamente las políticas de seguridad informáticas en una organización se corren muchos riesgos. A continuación se describe las fases para poder conocer el riesgo en una organización con políticas débiles.

3.9.1. Análisis de riesgos

El término análisis de riesgos hace referencia al proceso necesario para responder ciertas preguntas básicas:

- Se debe poder obtener una evaluación económica del impacto de estos sucesos. Este valor se podrá utilizar para contrastar el costo de la protección de la información en análisis, versus el costo de volverla a producir (reproducir).

- Se debe tener en cuenta la probabilidad que sucedan cada uno de los problemas posibles. De esta forma se pueden priorizar los problemas y su costo potencial desarrollando un plan de acción adecuado.
- Se debe conocer qué se quiere proteger, dónde, cómo, y contra quien, asegurando que con los costos en los que se incurren se obtengan beneficios efectivos. Para esto se deberá identificar los recursos (hardware, software, información, personal, accesorios, etc.) con que se cuenta y las amenazas a las que se está expuesto.

Tras analizar y evaluar los riesgos a los que nos enfrentamos podremos implementar las soluciones prácticas para minimizar sus efectos.

3.9.2. Evaluación del riesgo.

La evaluación de riesgos y presentación de respuestas debe prepararse de forma personalizada para cada organización; pero se puede plantear algunas preguntas que ayudan en la identificación del problema como por ejemplo:

- ¿Qué puede ir mal?”
- ¿Con qué frecuencia puede ocurrir?”
- ¿Cuáles serían sus consecuencias?”
- ¿Qué fiabilidad tienen las respuestas a las tres primeras preguntas?”
- ¿Se está preparado para abrir las puertas del negocio sin sistemas, por un día, una semana, cuanto tiempo?”
- ¿Cuál es el costo de una hora sin procesar, un día, una semana...?”
- ¿Cuánto, tiempo se puede estar off–line sin que los clientes se vayan a la competencia?”
- ¿Se tiene forma de detectar a un empleado deshonesto en el sistema?”
- ¿Se tiene control sobre las operaciones de los distintos sistemas?”
- ¿Cuantas personas dentro de la empresa, (sin considerar su honestidad), están en condiciones de inhibir el procesamiento de datos?”

- ¿A que se llama información confidencial y/o sensitiva?”
- ¿La información confidencial y sensitiva permanece así en los sistemas?”
- ¿La seguridad actual cubre los tipos de ataques existentes y está preparada para adecuarse a los avances tecnológicos esperados?”
- ¿A quien se le permite usar que recurso?”
- ¿Quién es el propietario del recurso? y ¿quién es el usuario con mayores privilegios sobre ese recurso?”
- ¿Cuáles serán los privilegios y responsabilidades del Administrador vs. la del usuario?”
- ¿Cómo se actuará si la seguridad es violada?”

Una vez obtenida la lista de cada uno de los riesgos se efectuará un resumen como el siguiente:

Tipo de Riesgo	**Factor**
Robo de hardware	Alto
Robo de información	Alto
Vandalismo	Medio
Fallas en los equipos	Medio
Virus Informáticos	Medio
Equivocaciones	Medio
Accesos no autorizados	Medio
Fraude	Bajo
Fuego	Muy Bajo
Terremotos	Muy Bajo

Tabla 3.1 tipo de riesgo y su severidad.

Según esta tabla habrá que tomar las medidas pertinentes de seguridad para cada caso en particular, cuidando incurrir en los costos necesarios según el factor de riesgo representado.

3.9.3. Niveles de riesgo.

Como puede apreciarse en la tabla los riesgos se clasifican por su nivel de importancia y por la severidad de su pérdida:

- Estimación del riesgo de pérdida del recurso (Ri)
- Estimación de la importancia del recurso (Ii)

Para la cuantificación del riesgo de perder un recurso, es posible asignar un valor numérico de 0 a 10, tanto a la importancia del recurso (10 es el recurso de mayor importancia) como al riesgo de perderlo (10 es el riesgo más alto).

El riesgo de un recurso será el producto de su importancia por el riesgo de perderlo:

$$WR_i = R_i * I_i$$

Luego, con la siguiente fórmula es posible calcular el riesgo general de los recursos de la red:

$$W_R = \frac{(WR_1 * I_1 + WR_2 * I_2 + ...+ WR_n * I_n)}{(I_1 + I_2 +...+ I_n)}$$

Otros factores que debe considerar para el análisis de riesgo de un recurso de red son su disponibilidad, su integridad y su carácter confidencial, los cuales pueden incorporarse a la fórmula para ser evaluados.

Ejemplo: el Administrador de una red ha estimado los siguientes riesgos y su importancia para los elementos de la red que administra:

Recurso	**Riesgo (R_i)**	**Importancia (I_i)**	**Riesgo Evaluado (R_i*I_i)**
Router	6	7	42
Gateway	6	5	30

Servidor	10	10	100
PC's	9	2	18

Tabla 3.2 Evaluación de Riesgos

Aquí ya puede apreciarse que el recurso que más debe protegerse es el servidor. Para la obtención del riesgo total de la red calculamos:

$$W_R = \frac{42 + 30 + 100 + 18}{7 + 5 + 10 + 2} = 7.92$$

Al ver que el riesgo total de la red es de casi 8 puntos sobre 10 debería pensarse seriamente en buscar las probables causas que pueden provocar problemas a los servicios brindados por los elementos evaluados.

3.9.4. Identificación de amenaza.

Una vez conocidos los riesgos, los recursos que se deben proteger y como su daño o falta pueden influir en la organización es necesario identificar cada una de las amenazas y vulnerabilidades que pueden causar estas bajas en los recursos. Como ya se mencionó existe una relación directa entre amenaza y vulnerabilidad a tal punto que si una no existe la otra tampoco.

Se debería disponer de una lista de amenazas (actualizadas) para ayudar a los administradores de seguridad a identificar los distintos métodos, herramientas y técnicas de ataque que se pueden utilizar. Es importante que los Administradores actualicen constantemente sus conocimientos en esta área, ya que los nuevos métodos, herramientas y técnicas para sortear las medidas de seguridad evolucionan de forma continua.

3.9.5. Evaluación de costos.

Desde un punto de vista oficial, el desafío de responder la pregunta del valor de la información ha sido siempre difícil, y más difícil aún hacer estos costos justificables, siguiendo el principio que “si desea justificarlo, debe darle un valor”.

Establecer el valor de los datos es algo totalmente relativo, pues la información constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, la documentación o las aplicaciones. Además, las medidas de seguridad no influyen en la productividad del sistema por lo que las organizaciones son reticentes a dedicar recursos a esta tarea. Por eso es importante entender que los esfuerzos invertidos en la seguridad son costeables.

La evaluación de costos más ampliamente aceptada consiste en cuantificar los daños que cada posible vulnerabilidad puede causar teniendo en cuenta las posibilidades. Un planteamiento posible para desarrollar esta política es el análisis de lo siguiente:

- ¿Qué recursos se quieren proteger?
- ¿De qué personas necesita proteger los recursos?
- ¿Qué tan reales son las amenazas?
- ¿Qué tan importante es el recurso?
- ¿Qué medidas se pueden implantar para proteger sus bienes de una manera económica y oportuna?

Con esas sencillas preguntas (más la evaluación de riesgo) se debería conocer cuáles recursos vale la pena (y justifican su costo) proteger, y entender que algunos son más importantes que otros.

El objetivo que se persigue es lograr que un ataque a los bienes sea más costoso que su valor, invirtiendo menos de lo que vale. Para esto se define tres costos fundamentales:

- **CP:** Valor de los bienes y recursos protegidos.

- **CR:** Costo de los medios necesarios para romper las medidas de seguridad establecidas.

- **CS:** Costo de las medidas de seguridad.

Para que la política de seguridad sea lógica y consistente se debe cumplir que:

- **CR > CP**: esto significa que un ataque para obtener los bienes debe ser más costoso que el valor de los mismos. Los beneficios obtenidos de romper las medidas de seguridad no deben compensar el costo de desarrollo del ataque.
- **CP > CS:** significa que el costo de los bienes protegidos debe ser mayor que el costo de la protección. Luego, **CR > CP > CS** y lo que se busca es:

- "**Minimizar** el costo de la protección manteniéndolo por debajo del de los bienes protegidos". Si proteger los bienes es más caro de lo que valen, entonces resulta más conveniente obtenerlos de nuevo en vez de protegerlo.
- "**Maximizar** el costo de los ataques manteniéndolo por encima del de los bienes protegidos". Si atacar el bien es más caro de lo que valen, al atacante le conviene más obtenerlo de otra forma menos costosa.

Se debe tratar de valorar los costos en que se puede incurrir en el peor de los casos contrastando con el costo de las medidas de seguridad adoptadas. Se debe poner especial énfasis en esta etapa para no incurrir en el error de no considerar costos, muchas veces, ocultos y no obvios (costos derivados).

3.9.6. Valor intrínseco.

Es el más fácil de calcular ya que solo consiste en otorgar un valor a la información contestando preguntas como las mencionadas y examinando minuciosamente todos los componentes a proteger.

3.9.7. Costos derivados de la pérdida.

Una vez más deben abarcarse todas las posibilidades, intentando descubrir todos los valores derivados de la pérdida de algún componente del sistema. Muchas veces se trata del valor añadido que gana un atacante y la repercusión de esa ganancia para el entorno, además del costo del elemento perdido. Deben considerarse elementos como:

- Información aparentemente inocua como datos personales, que pueden permitir a alguien suplantar identidades.
- Datos confidenciales de acuerdos y contratos que un atacante podría usar para su beneficio.
- Tiempos necesarios para obtener ciertos bienes. Un atacante podría acceder a ellos para ahorrarse el costo (y tiempo) necesario para su desarrollo.

3.10. ESTABLECIENDO POLÍTICAS ESTRATÉGICAS.

Para establecer una estrategia adecuada es conveniente pensar una política de protección en los distintos niveles que esta debe abarcar y que no son ni mas ni menos que los factores siguientes: Físico, Lógico, Humana y la interacción que existe entre estos.

En cada caso considerado, el plan de seguridad debe incluir una estrategia Proactiva y otra Reactiva.

- **La estrategia proactiva** (proteger y proceder) o previsión de ataques. es un conjunto de pasos que ayuda a reducir al mínimo la cantidad de puntos vulnerables existentes en las directivas de seguridad y a desarrollar planes de contingencia. La determinación del daño que un ataque va a provocar en un sistema y las debilidades y puntos vulnerables explotados durante este ataque ayudará a desarrollar esta estrategia

- **La estrategia reactiva** (perseguir y procesar) o estrategia posterior al ataque. Ayuda al personal de seguridad a evaluar el daño que ha causado el ataque, a repararlo o a implementar el plan de contingencia desarrollado en la estrategia Proactiva, a documentar y aprender de la experiencia, y a conseguir que las funciones comerciales se normalicen lo antes posible.

Con respecto a la postura que puede adoptarse ante los recursos compartidos:

- **Lo que no se permite expresamente está prohibido**: significa que la organización proporciona una serie de servicios bien determinados y documentados, y cualquier otra cosa está prohibida.
- **Lo que no se prohíbe expresamente está permitido**: significa que, a menos que se indique expresamente que cierto servicio no está disponible, todos los demás sí lo estarán.

Estas posturas constituyen la base de todas las demás políticas de seguridad y regulan los procedimientos puestos en marcha para implementarlas. Se dirigen a describir qué acciones se toleran y cuáles no.

Actualmente, los expertos se inclinan por recomendar la primera política mencionada. La cual es la estrategia proactiva.

3.11. IMPLEMENTACIÓN.

La implementación de medidas de seguridad, es un proceso Técnico–Administrativo. Debido a que se abarcar toda la organización, sin exclusión alguna, debe estar fuertemente apoyado por el sector gerencial, ya que sin ese apoyo, las medidas que se tomen no tendrán la fuerza necesaria.

Se debe tener en cuenta que la implementación de Políticas de Seguridad, trae varios tipos de problemas que afectan el funcionamiento de la organización. La

implementación de un sistema de seguridad conlleva a incrementar la complejidad en la operabilidad de la organización, tanto técnica como administrativa.

Por esto, será necesario medir cuidadosamente la ganancia en seguridad respecto de los costos administrativos y técnicos que se generen.

Es fundamental no dejar de lado la notificación a todos los involucrados en las nuevas disposiciones y, darlas a conocer con el fin de otorgar visibilidad a los actos de la administración.

Una PSI informática deberá abarcar:

- Alcance de la política, incluyendo sistemas y personal sobre el cual se aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidad de cada uno de los servicios, recurso y responsables en todos los niveles de la organización.
- Responsabilidades de los usuarios con respecto a la información que generan y a la que tienen acceso.
- Requerimientos mínimos para la configuración de la seguridad de los sistemas al alcance de la política.
- Definición de violaciones y las consecuencias del no cumplimiento de la política.
- Por otra parte, la política debe especificar la autoridad que debe hacer que las cosas ocurran, el rango de los correctivos y sus actuaciones que permitan dar indicaciones sobre la clase de sanciones que se puedan imponer. Pero, no debe especificar con exactitud qué pasara o cuándo algo sucederá; ya que no es una sentencia obligatoria de ley.
- Explicaciones comprensibles (libre de tecnicismos y términos legales pero sin sacrificar su precisión) sobre el porque de las decisiones tomadas.
- Finalmente, como documento dinámico de la organización, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales

relevantes: crecimiento de la planta de personal, cambio en la infraestructura computacional, alta y rotación de personal, desarrollo de nuevos servicios, cambio o diversificación de negocios, etc.

3.12. AUDITORÍA Y CONTROL.

Se considera que la auditoria son los “ojos y oídos” de la dirección, que generalmente no puede, no sabe o no debe realizar las verificaciones y evaluaciones.

La auditoria consiste en contar con los mecanismos para poder determinar qué es lo que sucede en el sistema, qué es lo que hace cada uno y cuando lo hace.

En cuanto al objetivo del Control es contrastar el resultado final obtenido contra el deseado, a fin de incorporar las correcciones necesarias para alcanzarlo, o bien verificar la efectividad de lo obtenido.

3.13. LA POLÍTICA.

Los fundamentos aquí expuestos **no deben** ser tomados puntualmente en cada organización tratada. Deberán ser adaptados a la necesidad, requisitos y limitaciones de cada organización o usuario individual y, posteriormente requerirá actualizaciones periódicas asegurando el dinamismo sistemático que genera cada organización.

3.13.1. Nivel físico.

El primer factor considerado, y el más evidente debe ser asegurar la esencia del objeto a proteger. Es preciso establecer un perímetro de seguridad a proteger, y esta protección debe adecuarse a la importancia de lo protegido.

La defensa contra agentes nocivos conlleva tanto medidas proactivas (limitar el acceso) como normativas de contingencia (que hacer en caso de incendio) o

medidas de recuperación (realizar copias de seguridad). El grado de seguridad solicitado establecerá las necesidades: desde el evitar el café y el tabaco en las proximidades de equipos electrónicos, hasta el establecimiento de controles de acceso a la sala de equipos.

Lo más importante es recordar que quien tiene acceso físico a un equipo tiene control absoluto del mismo. Por ello sólo deberían accederlo aquellas personas que sean estrictamente necesarias.

a. Amenaza no intencionada (desastre natural)

El siguiente ejemplo ilustra una posible situación:

Una organización no cuenta con sistemas de detección y protección de incendios en la sala de servidores. El Administrador del sistema deja unos papeles sobre el aire acondicionado de la sala. Durante la noche el acondicionador se calienta y se inicia un incendio que termina con la sala de servidores y un par de despachos contiguos.

Directivas:

- **Predecir Ataque/Riesgo:** Incendio.
- **Amenaza:** Desastre natural.
- **Ataque:** No existe.
- **Estrategia Proactiva:**
    - a. Predecir posibles daños: pérdida de equipos e información.
    - Determinar y minimizar vulnerabilidades: protección contra incendios.
    - Evaluar planes de contingencia: backup de la información.
- **Estrategia Reactiva:**
    - Evaluar daños: perdida de hardware e información.
    - Determinar su origen y repararlos: bloqueo del aire acondicionado.
    - Documentar y aprender.
    - Implementar plan de contingencia: recuperar backups.

- **Examinar resultados y eficacia de la directiva:** Ajustar la directiva con los nuevos conceptos incorporados.

3.13.2 Factor humano.

El factor humano como se ha mencionado juega un papel importante en la seguridad.

Quizás el usuario contempla todas las noticias de seguridad con escepticismo, piensan que los Administradores son paranoicos y se aprovechan de las contadas situaciones dadas. Quizás tengan razón, pero se debe recordar que el mundo virtual no es más que una pequeña muestra del mundo físico, con el agregado que es el campo ideal de impunidad y anonimato.

Generalmente se sobre valora la capacidad de un atacante. Al contrario de la creencia popular no se necesita ser un Gurú para ingresar en una computadora y generalmente quienes lo hace son Script–Kiddies. La pregunta ya no es ¿seré atacado?; sino ¿cuándo seré atacado?.

a. Amenaza no Intencionada (Empleado)

El siguiente ejemplo ilustra una posible situación de contingencia y el procedimiento a tener en cuenta:
Un empleado, no desea perder la información que ha guardado en su disco rígido, así que la copia a su carpeta particular del servidor, que resulta ser también el servidor principal de aplicaciones de la organización. No se han definido cuotas de disco para las carpetas particulares de los usuarios que hay en el servidor. El disco rígido del usuario tiene 6 GB de información y el servidor tiene 20 GB. Sumando todo lo guardado de los demás usaros solo queda libre 0.5 GB del espacio total. El servidor de aplicaciones deja de responder a las actualizaciones y peticiones porque se ha quedado sin espacio en el disco. El resultado es que se deniega a los usuarios los servicios del servidor de aplicaciones y la productividad se interrumpe.

A continuación, se explica la metodología que se debería haber adoptado antes de que el usuario decida realizar su copia de seguridad:

Directivas:

- **Predecir Ataque/Riesgo:** Negación de servicios por abuso de recursos.
- **Amenaza:** No existe. Empleado sin malas intenciones.
- **Ataque:** No existe motivo ni herramienta, solo el desconocimiento por parte del usuario.
- **Estrategia Proactiva:**
    - Predecir posibles daños: pérdida de productividad por espacio de disco.
    - Determinar y minimizar vulnerabilidades: implementar cuotas de discos.
    - Evaluar planes de contingencia: servidor backup.
    - Capacitar el usuario.

- **Estrategia Reactiva:**
    - Evaluar daños: pérdida de producción.
    - Determinar su origen y repararlos: hacer espacio en el disco.
    - Documentar y aprender: implementar plan de contingencia.
- **Examinar resultados y eficacia de la directiva:** Ajustar la directiva con los nuevos conceptos incorporados.

b. Amenaza malintencionada.

Una empresa competidora ofrece a un usuario cierta suma de dinero para obtener el diseño del último producto desarrollado por su empresa. Como este usuario carece de los permisos necesarios para obtener el diseño se hace pasar como un Administrador, de esta manera consigue el nombre de usuario y password de un usuario con los permisos que él necesita.

La política de seguridad asociada a este evento debería haber contemplado:

Directivas:

- **Predecir Ataque/Riesgo:** Robo de información mediante el uso de ingeniería social.
- **Amenaza:** Insider.
- **Ataque:** Ingeniería social.
- **Estrategia Proactiva:**
    - Predecir posibles daños: pérdida de productividad y/o beneficios.
    - Determinar y minimizar vulnerabilidades: concientización de los usuarios.
    - Evaluar planes de contingencia.
- **Estrategia Reactiva:**
    - Evaluar daños: pérdida de beneficios e información.
    - Determinar su origen: revelación de login y password por parte el usuario.
    - Reparación de daños: implementar entrenamiento de los usuarios.
    - Documentar y aprender.
    - Implementar plan de contingencia.
- **Examinar resultados y eficacia de la directiva:** Ajustar la directiva con los nuevos conceptos incorporados.

3.13.3. Personas ajenas al sistema.

Este tipo de personas también pueden ocasionar daños a la organización ya sea se una forma intencionada o no.

a. Amenaza no intencionada

Un virus ingresa a la empresa mediante un mail enviado a un empleado, y comienza a expandirse dentro de la misma tomando como base la libreta de direcciones de los usuarios:

Directivas:

- **Predecir Ataque/Riesgo:** Negación de servicio del servidor de correo electrónico por gran la cantidad de mensajes enviados/recibidos.
- **Amenaza:** Virus.
- **Ataque:** Virus de correo electrónico.
- **Estrategia Proactiva:**
    - Predecir posibles daños: pérdida de productividad por negación de servicio.
    - Determinar y minimizar vulnerabilidades: actualización de antivirus y concientización de usuarios en el manejo del correo electrónico.
    - Evaluar planes de contingencia: evaluar la importancia de un servidor backup. Antivirus.
- **Estrategia Reactiva:**
    - Evaluar daños: pérdida de producción.
    - Determinar su origen: caída del servidor por overflow de mensajes.
    - Reparación de daños: implementar el servidor backup. Eliminación del virus causante del problema.
    - Documentar y aprender.
    - Implementar plan de contingencia: servidor backup.
- **Examinar resultados y eficacia de la directiva:** Ajustar la directiva con los nuevos conceptos incorporados.

b. Amenaza malintencionada (out–sider)

Una persona ingresa al sistema de la empresa, con intenciones de recopilar información para su posterior venta:

Directivas:

- **Predecir Ataque/Riesgo:** Ingreso al sistema por vulnerabilidades en los sistemas o política de claves ineficiente.

- **Amenaza:** Outsider recopilando información significativa.
- **Ataque:** Ingreso al sistema.
- **Estrategia Proactiva:**
    - Predecir posibles daños: Robo y venta de información. Daño a la imagen de la empresa.
    - Determinar y minimizar vulnerabilidades: actualización de sistemas vulnerables. Concientización a los usuarios en el manejo de contraseñas fuertes.
    - Evaluar planes de contingencia: implementación de servidor backup para casos de daño de la información. Recuperación de imagen. Evaluar formas de minimizar el daño por la información robada.
- **Estrategia Reactiva:**
    - Evaluar daños: información susceptible robada.
    - Determinar su origen: ingreso al sistema.
    - Reparación de daños.
    - Documentar y aprender.
    - Implementar plan de contingencia: servidor backup.
- **Examinar resultados y eficacia de la directiva:** Ajustar la directiva con los nuevos conceptos incorporados.

3.14 POLÍTICAS DE LA RED CORPORATIVA.

Las áreas que controlaran las políticas y las normas de la red corporativa serán las siguientes:

- La administración de las áreas de informática.
- Responsables de la seguridad, comunicación, y soporte técnico.
- Comisión encargada del software y hardware.

3.14.1 Políticas generales.

A continuación se detallan las políticas generales.

- La Administración de la red interna, la seguridad de los equipos y los sistemas de la Red Corporativa serán responsabilidad de la gerencia de informática.
- El estudio del crecimiento o reubicación de la red interna de la organización será, correspondiente al área de informática.
- La gestión y resolución de fallas en la Red Interna, Seguridad, y Servidores será responsabilidad de los administradores de cada área.
- La responsabilidad de los administradores del área correspondiente es de implementar prácticas que tengan como fin la habilitación de servicios, soporte y mantenimiento de la red local.
- Los nombres asignados a cada Pc y a las cuentas de los usuarios de la red corporativa contaran con estándares de identificación.
- Todo tipo de acceso a la red corporativa deberá ser gestionado y autorizado a través de la Gerencia informática.

3.14.2 Control de acceso a usuarios.

A continuación se describen ciertas políticas.

a. Administración de accesos.

1. Para el acceso a información de la red corporativa será necesario estar debidamente autorizado a través de usuarios y contraseñas.
2. La gerencia informática decidirá el esquema de seguridad para las aplicaciones que utiliza especificando los roles genéricos y la asignación de los usuarios.
3. La gerencia informática es la responsable de asignar correctamente el acceso a los usuarios de acuerdo al perfil autorizado.

4. Si un departamento de la organización necesita agregar nuevos usuarios a ciertas aplicaciones deberá mandar una solicitud de adición de usuarios al departamento de administración de dicha aplicación debidamente firmado.
5. El monitoreo de Sistemas será responsabilidad de cada Administración con el objetivo de identificar y dar seguimiento a accesos no autorizados, anormales o irregulares.
6. Queda prohibido, la prueba o el uso de cualquier tipo de software o técnica con fin de violar la seguridad de los sistemas.
7. Las cuentas bloqueadas podrán ser habilitadas nuevamente después que jefe inmediato envié una solicitud al administrador de dicha aplicación.

b. Accesos remotos

1. El acceso remoto a la red corporativa se implementará a través de mecanismos de autenticación, mediante la asignación de cuentas de uso a usuarios, no traspasables a terceros.
2. Los usuarios deberán, cumplir con las mismas normas que los usuarios de la red interna, deberán tener mucho cuidado con las contraseñas de acceso a la red.
3. El equipo utilizados por los usuarios remotos tendrán que cumplir con las normas de seguridad de la red corporativa.
4. El mal uso o traspaso de la cuenta de acceso remoto a terceros, sin autorización, originará sanciones cuya severidad y alcance será determinado por la junta directiva de la red corporativa, dependiendo el impacto que la acción pueda originar.
5. Para transferir datos sensibles a través de conexiones remotas, se utilizara métodos de encriptación en ambos extremos de la comunicación
6. Las conexiones remotas que no se estén empleando, en un periodo 60 días, serán deshabilitados.

c. Accesos de terceros

1. Los accesos a todas las terceras personas, a los servicios o sistemas de la red corporativa, estarán sujetos a las restricciones y normas indicadas por la organización.
2. Se creara un contrato estableciendo las directrices en caso de violar la información sensitiva que maneja la organización.
3. La falta del cumplimiento de las normas y políticas de seguridad de la información será objeto de una investigación llevando a establecer demandas judiciales.
4. Los accesos de terceros siempre serán asignados en forma temporal, por períodos fijos, en caso se terminara el tiempo se enviaría una solicitud a gerencia de informática pidiendo un nuevo acceso.
5. Cada vez que terceras personas quieran conectarse a un recurso crítico de la red corporativa serán supervisados por personal interno de la organización.

d. Caducidad de permisos de acceso

1. Si el empleado deja de trabajar por diferentes circunstancias los permisos de acceso a la red corporativa se cancelaran de inmediato.
2. El acceso a la red corporativa será suspendido cuando se encuentren inactivos por más de 60 días, y el jefe inmediato no lo haya reportado.
3. Para el empleado de la organización las contraseñas estarán vigentes por un máximo de un mes.
4. Las solicitudes de baja de acceso a sistemas de información debe ser notificada por el jefe inmediato del usuario que será dado de baja,
5. Las cuentas y claves de los usuarios administradores de los sistemas, deberán estar impresos, resguardados en un sobre en un lugar que garantice la confidencialidad de dicha información bajo la responsabilidad de la gerencia de informática.

6. En caso de accesos fallidos a la red, el sistema de seguridad deberá mantener dicha información en detalle con el nombre del usuario, fecha, aplicación, archivos, a los que pretendía acceder, así como también el número de intentos.

e. Uso de claves de acceso.

1. Todo usuario que tenga acceso a estaciones de trabajo, acceso remoto, o cualquier otro servicio dependiente de la red corporativa, utilizará claves de acceso personales, no compartidas.
2. El usuario tendrá el control total de cambiar su clave de acceso al sistema ya sea cuando se le este venciendo el plazo o cuando ingrese por primera vez al sistema.
3. Todo usuario debe ser totalmente responsable, tanto del uso de su cuenta de usuario como de la respectiva contraseña,
4. La clave secreta para los usuarios debe cumplir con un estándar el cual es el siguiente:

    - Largo mínimo de ocho caracteres.
    - Debe tener por lo menos tres caracteres especiales
    - No debe tener relación con el sistema, con el nombre del usuario, algún alias de del usuario.
    - Se establecerá un periodo de 30 días como máximo para el cambio obligatorio de la clave.

Nota: las claves que ya fueron utilizadas no podrán utilizarse nuevamente.

3.14.3 Política de respaldos.

1. Los respaldos de información deben realizarse en forma ordenada que asegure que toda la información necesaria estará disponible incluso ante un

evento de completa destrucción.

2. Los respaldo deberán quedar protegidos de accesos de terceros, daños, hurtos, siniestros, manipulaciones. para cumplir esta política se deberán almacenar en un lugar especial, donde se registrara la persona que ingreso o saco él medio,
3. Todos los respaldos deben ser probados periódicamente para verificar que cumplen con el objetivo de recuperar toda la información. Responsabilidad del administrador del servidor o de la aplicación.
4. La política de respaldo contemplará tener dos copias de los respaldos. Uno de los respaldos debe obligadamente ser almacenada en un lugar externo al edificio donde se encuentre el equipo de cómputo.
5. Se deberán implementar controles operativos para asegurar que el proceso de respaldo ha sido ejecutado de manera correcta y sin fallas.
6. Los respaldos sólo podrán ser manipulados, almacenados o recuperados por una persona asignada a cumplir esta función.
7. Aquellos usuarios que respalden información del Negocio en disquetes, cintas, o cualquier medio local de su estación de trabajo, deberá estar autorizado por el jefe inmediato.

3.14.4 Política del uso del software.

1. La gerencia informática tendrá un registro permanente, del equipo y del software instalado en sus servidores y estaciones de trabajo, con el fin de mantener un adecuado control.
2. No se permite que personas no autorizadas hagan uso de software que afecte la seguridad de la corporación.
3. Solamente se hará uso de software que este debidamente autorizado por la gerencia informática.

3.14.5. Política del Internet.

1. El uso de Internet deberá estar orientado al cumplimiento de las actividades

laborales de cada empleado, sin embargo estará permitido el uso con fines personales, siempre que éstos no interfieran con las funciones laborales de dicha persona.

2. Estará prohibido a los usuarios y personal técnico instalar o probar software bajado de Internet, aún siendo este gratis y de libre circulación.
3. La gerencia informática es la encargada de la restricción de páginas de navegación que atenten contra la moralidad de los empleados o la seguridad.
4. El uso indebido de este recurso, estará sujeto a sanciones que serán desde el descuento en el salario hasta la suspensión del contrato.
5. Se deberá controlar la introducción de virus que pudiera producirse en forma intencional o bien accidentalmente, a través de archivos bajados desde Internet.
6. Se prohíbe la utilización del Internet para manejar o participar en actividades donde se compromete la información de la corporación, estar involucrado en actividades fraudulentas, o distribuir intencionalmente información falsa.

CAPITULO 4. SEGURIDAD DEL ENTORNO DE OPERACIONES

Es el primer paso en la estrategia de seguridad “defensa en profundidad”. Ya que su aporte es esencial e importante en las corporaciones. No se puede hablar de seguridad sino no se tiene el entorno de operaciones seguro, por esta razón se debe tomar en cuenta los siguientes elementos: la seguridad física, protección del hardware y la protección de los datos.

Puntos clave.

- Describe la seguridad física

- Describe como proteger el hardware por medio de políticas de seguridad en caso de desastres naturales o por desastres causados por el entorno.

- Menciona algunas técnicas de protección del equipo en caso de los desastres naturales o por desastres causados por el entorno.

4.1 SEGURIDAD FÍSICA.

La seguridad física de los sistemas informáticos consiste en la aplicación de barreras físicas y procedimientos de control como medidas de prevención a las amenazas de los recursos y la información confidencial. Más claramente, por seguridad física podemos entender todos aquellos mecanismos generalmente de prevención y detección destinados a proteger físicamente cualquier recurso del sistema; estos recursos son desde un simple teclado hasta una cinta de backup con toda la información que hay en el sistema, pasando por la propia CPU de la máquina.

4.2 PROTECCIÓN DEL HARDWARE.

El hardware es frecuentemente el elemento más caro de todo el sistema informático. Por tanto, las medidas encaminadas a asegurar su integridad son: una parte importante de la seguridad física de cualquier organización, especialmente las que tienen redes de comunicación. Algunas suelen poseer entre sus equipos máquinas muy caras, desde servidores con una gran potencia de cálculo hasta routers de última tecnología, pasando por modernos sistemas de transmisión de datos como: la fibra óptica.

Son muchas las amenazas al hardware de una organización; aquí se van a presentar algunas de ellas, sus posibles efectos y algunas soluciones, no para evitar los problemas sí al menos para minimizar sus efectos.

4.2.1 Acceso físico.

La posibilidad de acceder físicamente a una máquina que tenga cualquier sistema operativo hace inútiles casi todas las medidas de seguridad que hayamos aplicado sobre ella: tenemos que pensar que si un atacante puede llegar con total libertad hasta una servidor o al centro de informática de una organización puede por ejemplo: abrir el CPU y llevarse un disco duro; sin necesidad de privilegios en el sistema, sin

importar la robustez de nuestros cortafuegos, sin utilizar una clave de usuario. Seguramente el atacante podrá modificar la información almacenada, destruirla o simplemente leerla. Incluso sin llegar al extremo de desmontar la máquina.

La persona que accede al equipo puede parar o arrancar una versión diferente del sistema operativo sin llamar mucho la atención. Si por ejemplo alguien accede a un departamento informático con máquinas Linux, seguramente le resultará fácil utilizar un disco de arranque, montar los discos duros de la máquina y extraer de ellos la información deseada; incluso es posible que utilice un ramdisk con ciertas utilidades que constituyen una amenaza para otros equipos, como nukes o sniffers.

Cierta seguridad física es necesaria para garantizar la seguridad global de la red y de los sistemas conectados a ella; evidentemente el nivel de seguridad física depende completamente del entorno donde se ubiquen los puntos a proteger. Como por ejemplo: los servidores de una organización o las máquinas de los despachos.

a. Prevención.

¿Cómo prevenir un acceso físico no autorizado a un determinado punto? Hay soluciones para todos los gustos, y también de todos los precios: desde analizadores de retina hasta videocámaras, pasando por tarjetas inteligentes o control de las llaves que abren determinada puerta. Todos los modelos de autenticación de usuarios son aplicables para: controlar el acceso lógico a los sistemas y el acceso físico; de todos ellos, quizás los más adecuados a la seguridad física sean los biométricos; aunque resulten caro para utilizarlos masivamente en entornos de seguridad media.

Pero no hay que irse a sistemas tan complejos para prevenir accesos físicos no autorizados; normas tan elementales como cerrar las puertas con llave al salir de un departamento, un despacho o bloquear las tomas de red que no se suelan utilizar y que estén situadas en lugares apartados son en ocasiones más que suficientes para prevenir ataques.

Uno de los elementos importantes para la seguridad es el cableado de red. Por lo que es recomendable apartarlo del acceso directo; por desgracia, en muchas organizaciones podemos ver excelentes ejemplos de lo que no hay que hacer en este sentido: cualquiera organización que tenga una infraestructura más o menos grande por ejemplo: el campus de una universidad, seguramente podrá ver, pinchar o cortar los cables que se encuentran al alcance de todo el mundo.

Todos hemos visto películas en las que se mostraba un estricto control de acceso a instalaciones militares mediante tarjetas inteligentes, analizadores de retina o verificadores de la geometría de la mano; aunque algunos de estos métodos aún suenen a ciencia ficción y sean demasiado caros para la mayor parte de entornos (recordemos que si el sistema de protección es más caro que lo que se quiere proteger tenemos un grave error en nuestros planes de seguridad), otros se pueden aplicar, en muchas organizaciones.

Concretamente, el uso de lectores de tarjetas para poder acceder a ciertas dependencias es algo muy a la orden del día; la idea es sencilla: alguien pasa una tarjeta por el lector, que conecta con un sistema por ejemplo: un ordenador en el que exista una base de datos con información de los usuarios y los recintos a los que se le permite el acceso. Si la tarjeta pertenece a un usuario capacitado para abrir la puerta, ésta se abre, y en caso contrario se registra el intento y se niega el acceso.

Este método quizás resulte un poco caro para extenderlo a todos y cada uno de los puntos a proteger en una organización, sin embargo no sería tan descabellado instalar pequeños lectores de códigos de barras conectados a una máquina en las puertas de muchas áreas, especialmente en las que se maneja información más o menos sensible.

Estos lectores podrían leer una tarjeta en donde todos los miembros autorizados de la organización tendrían. Está tarjeta se desliza por el lector conectando con la base de datos de usuarios, y así autorizar o denegar la apertura de la puerta.

Se trataría de un sistema sencillo de implementar, no muy caro, y que cubre las necesidades de seguridad en la mayoría de entornos, incluso se podría disminuir costo de utilizar un mecanismo para abrir y cerrar puertas, si el sistema se limitara a informar al administrador del área o a un guardia de seguridad mediante un mensaje en la pantalla o una luz encendida. De esta forma los únicos gastos serían los correspondientes a los lectores de códigos de barras, ya que con el equipo y la base de datos se puede utilizar una máquina o un servidor de propósito general.

b. Detección.

Cuando la prevención es difícil por cualquier motivo: técnico, económico, humano. Es deseable que un potencial ataque sea detectado cuanto antes, para minimizar así sus efectos. Aunque en la detección de problemas, generalmente de accesos físicos no autorizados, intervienen medios técnicos como: cámaras de vigilancia de circuito cerrado o alarmas, en entornos más normales, el esfuerzo en detectar estas amenazas se ha de centrar en las personas que utilizan los sistemas y en las que sin utilizarlos están relacionadas de cierta forma con ellos; sucede lo mismo que con la seguridad lógica: se ha de ver toda la protección como una cadena que falla si falla su eslabón más débil.

Es importante concienciar a todos de su papel en la política de seguridad del entorno; si por ejemplo un usuario autorizado detecta presencia de alguien de quien sospecha que no tiene autorización para estar en una determinada área, debe avisar inmediatamente al administrador o al responsable de los equipos, que a su vez puede avisar al servicio de seguridad si es necesario. No obstante, utilizar este servicio debe ser solamente un último recurso.

Generalmente en la mayoría de entornos no estamos tratando con terroristas, sino por fortuna con elementos mucho menos peligrosos. Si cada vez que se sospecha de alguien se avisa al servicio de seguridad esto puede repercutir en el ambiente de trabajo de los usuarios autorizados, ocasionando una cierta presión que no es en absoluto recomendable.

Es muy simple lo que se debería hacer por ejemplo preguntar: ¿puedo ayudarte en algo? Esto suele ser más efectivo a que se llame a un guardia para que solicite una identificación formal. Esto es especialmente recomendable en lugares de acceso restringido, como laboratorios de investigación o centros de cálculo, donde los usuarios habituales suelen conocerse entre ellos y es fácil detectar personas ajenas al entorno.

4.2.2 Desastres naturales.

En el anterior punto hemos hecho referencia a los accesos físicos no autorizados a zonas o a elementos que pueden comprometer la seguridad de los equipos o de toda la red; sin embargo, no son estas las únicas amenazas relacionadas con la seguridad física. Un problema que no suele ser tan habitual, pero que en caso de producirse puede acarrear gravísimas consecuencias son: los desastres naturales y su falta de prevención.

a. Terremotos.

Los terremotos son desastres naturales que posiblemente no ocurran en la mayoría de organizaciones ubicadas en ciertas áreas, simplemente por su localización geográfica. El Salvador se encuentra en una zona donde suelen producirse temblores que alcanzan magnitudes razonables que no causan daño en los equipos. Por lo tanto, no se usan medidas serias contra los movimientos sísmicos, ya que la probabilidad de que suceda es baja y no merece la pena invertir dinero para minimizar sus efectos.

Las medidas contra terremotos son excesivamente caras para la mayoría de organizaciones en El Salvador, evidentemente serían igual de caras en zonas como Los Ángeles, pero allí el costo estaría justificado por la alta probabilidad que se produzcan movimientos de magnitudes considerables.

No cuesta nada tomar ciertas medidas de prevención; por ejemplo, es muy recomendable no situar equipos delicados en superficies muy elevadas porque un

pequeño temblor puede tirar desde una altura considerable un equipo completo, que con toda probabilidad se rompería. Es conveniente y barato fijar los elementos más críticos como: los CPUs, monitores o los router. No es recomendable situar objetos pesados en superficies altas cercanas a los equipos, ya que podría caerse y romper los dispositivos.

Para evitar mayores consecuencias en los terremotos, es muy importante colocar el equipo lejos de las ventanas porque, si se produce un temblor pueden caer sobre el equipo. Además, situando el equipo alejado de las ventanas estamos dificultando las acciones de un potencial ladrón. Ya que si los dispositivos estuvieran cerca no tendría ningún problema en alargar el brazo para llevárselo.

Quizás hablar de terremotos en un trabajo dedicado a sistemas no significa que debemos entenderlos únicamente por grandes desastres que destrozan edificios y vías de comunicación; quizás sería más apropiado hablar de vibraciones, desde las más grandes que son: los terremotos hasta las más pequeñas como un simple motor cercano a los equipos.

Las vibraciones, incluso las más imperceptibles, pueden dañar seriamente cualquier elemento electrónico de nuestras máquinas, especialmente si se trata de vibraciones continuas: los primeros efectos pueden ser problemas con los cabezales de los discos duros o con los circuitos integrados que se dañan en las placas.

Para hacer frente a pequeñas vibraciones podemos utilizar plataformas de goma, de forma que la plataforma absorba la mayor parte de los movimientos; una regla común es evitar que entren en contacto equipos que poseen una electrónica delicada con hardware más mecánico, como las impresoras: estos dispositivos no paran de generar vibraciones cuando están en funcionamiento, por lo que situar un pequeño impresor encima del CPU de una máquina es una idea mala.

Como dicen algunos expertos en seguridad, el espacio en la sala de operaciones es un problema sin importancia comparado con las consecuencias de fallos en los discos duros o en la placa base de un ordenador.

b. Tormentas eléctricas.

Las tormentas eléctricas, generan subidas repentinas de tensión infinitamente superiores a las que pueda generar un problema en la red eléctrica. Si cae un rayo sobre la estructura metálica del edificio donde están situados nuestros equipos es casi seguro que podemos ir pensando en comprar otros nuevos; sin llegar a ser tan dramáticos, la caída de un rayo en un lugar cercano puede inducir un campo magnético lo suficientemente intenso como para destruir el hardware que se encuentra algunas veces protegido contra voltajes elevados.

Sin embargo, las tormentas poseen un lado positivo: son predecibles con alguna exactitud, lo que permite a un administrador parar sus máquinas y desconectarlas de la línea eléctrica. Entonces, ¿cuál es el problema? Aparte de las propias tormentas, el problema son los responsables de los equipos: la caída de un rayo es poco probable pero no imposible. Mucha gente ni siquiera ha visto caer cerca un rayo debido a que existen aparatos destinados justamente a atraer rayos de una forma controlada; tanto es así que, los administradores piensan o asumen que eso no les va a suceder nunca, y menos a sus equipos.

Son muy pocos los administradores que se molestan en parar las máquinas y desconectarlas ante una tormenta; si el fenómeno sucede durante las horas de trabajo y la tormenta es fuerte, quizás se hace, pero si sucede un sábado por la noche nadie va a ir a la sala de operaciones a proteger los equipos, además ninguna persona se habrá tomado la molestia de protegerlos por una simple previsión meteorológica. Todos debemos de tomar más en serio la naturaleza.

c. Inundaciones y humedad.

En ambientes extremadamente secos el nivel de electricidad estática es elevado, lo que, puede transformar un pequeño contacto entre una persona y un circuito, o entre

diferentes componentes de una máquina, un daño irreparable en el hardware o a la información. Cierto grado de humedad es necesario para un correcto funcionamiento de nuestras máquinas. No obstante, niveles de humedad elevados son perjudiciales para los equipos porque pueden producir condensación en los circuitos integrados, lo que origina cortocircuitos que evidentemente tienen efectos negativos sobre cualquier elemento electrónico de una máquina.

Controlar el nivel de humedad en los entornos habituales es algo innecesario, ya que por norma nadie ubica el departamento de informática en los lugares más húmedos o que presenten situaciones extremas. Es necesario en algunos casos utilizar alarmas que se activan al detectar condiciones donde la humedad sea poca o demasiada, especialmente en sistemas de alta disponibilidad o de altas prestaciones, donde un fallo en un componente puede ser crucial. Ciertos equipos son especialmente sensibles a la humedad, por lo que es conveniente consultar los manuales.

Cuando ya no se habla de una humedad sino de completas inundaciones, los problemas generados son mucho mayores. Casi cualquier medio: una máquina, una cinta, un router que entre en contacto con el agua queda automáticamente inservible, ya que los sistemas electrónicos generan cortocircuitos.
Contra las inundaciones la medida más efectiva es: la de prevención porque: podemos utilizar detectores de agua en el suelo o en suelos falsos de las salas de operaciones, y apagar automáticamente los sistemas en caso de que se activen. En casos severos es necesario tener activado un sistema automático que corte la corriente eléctrica.

Algo muy común es intentar sacar los equipos de una sala que se está empezando a inundar; esto, que a primera vista parece lógico, es el mayor error que se puede cometer si no hemos desconectado completamente el sistema eléctrico, ya que la mezcla de corriente y agua puede causar incluso la muerte a quien intente salvar el equipo. Por muy caro que sea el hardware o por muy valiosa que sea la información a proteger, nunca serán magnitudes comparables a la pérdida de vidas humanas. Otro error común relacionado con los detectores de agua es situar a los mismos en

un nivel superior que a los propios equipos a salvaguardar, incluso en el techo junto a los detectores de humo. En este caso cuando el agua llega al detector poco se puede hacer por las máquinas o la información que contienen.

Medidas de protección menos sofisticadas pueden ser: la instalación de un suelo falso por encima del suelo real, o simplemente tener la precaución de situar a los equipos con cierta elevación respecto al suelo, pero sin llegar a situarlos muy altos.

4.2.3. Desastres del entorno.

Entre los desastres del entorno se encuentran:

a. Electricidad.

Quizás los problemas más frecuentes en el entorno de trabajo son: los relacionados con el sistema eléctrico que alimenta nuestros equipos. Los cortocircuitos, picos de tensión, cortes de flujo son a diario una amenaza a la integridad tanto de nuestro hardware como de los datos que almacena o que circulan por él.

El problema mas común en las instalaciones modernas son las subidas de tensión, conocidas como picos porque: generalmente aumentan durante unas fracciones de segundo el voltaje que recibe un equipo hasta sobrepasar el límite aceptable que dicho equipo soporta. Lo normal es que estos picos apenas afecten al hardware o a los datos gracias a que en la mayoría de equipos hay fusibles instalados, elementos que se funden ante una subida de tensión y dejan de conducir la corriente, provocando que la máquina permanezca apagada.

Una medida efectiva y barata es utilizar tomas de tierra para asegurar aún más la integridad; estos mecanismos evitan los problemas de sobre tensión desviando el exceso de corriente hacia el suelo de una sala, edificio, o simplemente hacia cualquier lugar con voltaje nulo. Un toma de tierra sencillamente puede consistir de un buen conductor conectado al chasis de los equipos a proteger o de una varilla maciza, que se introduce en el suelo; el costo de la instalación es pequeño, especialmente si lo comparamos con las pérdidas que supondría un incendio que afecte a todos o a una parte de nuestros equipos.

Si se tiene un sistema protegido con los métodos anteriores, y la subida de tensión dura demasiado, o si es demasiado rápida, podemos sufrir daños en los equipos; existen acondicionadores de tensión comerciales que protegen de los picos hasta en los casos más extremos, y que también se utilizan como filtros para ruido eléctrico. Aunque en la mayoría de situaciones no es necesario su uso. Si nuestra organización tiene problemas por el voltaje excesivo quizás sea conveniente instalar alguno de estos aparatos.

Un problema que los estabilizadores de tensión o los toma de tierra no pueden solucionar es justamente: las bajadas, situaciones en las que la corriente desciende por debajo del voltaje necesario para un correcto funcionamiento del sistema, pero sin llegar a ser lo suficientemente bajo para que la máquina se apague. En estas situaciones la máquina se va a comportar de forma extraña e incorrecta, por ejemplo no aceptando algunas instrucciones, no completando escrituras en disco o memoria, etc. Es una situación similar a la de una bombilla que pierde intensidad momentáneamente por falta de corriente, pero trasladada a un sistema que en ese pequeño intervalo ejecuta miles o millones de instrucciones y transferencias de datos.

Otro problema muy habitual son: los cortes en el fluido eléctrico que llegan a nuestros equipos. Aunque un simple corte de corriente no suele afectar al hardware, lo más peligroso son las idas y venidas rápidas de la corriente; en esta situación, aparte de perder datos, nuestras máquinas pueden sufrir daños.

La forma más efectiva de proteger nuestros equipos contra estos problemas de la corriente eléctrica es: utilizar una SAI (Servicio de Alimentación Ininterrumpido) conectado al elemento que queremos proteger. Estos dispositivos mantienen un flujo de corriente correcto y estable, protegiendo así los equipos de las subidas, los cortes y bajadas de tensión. Estos dispositivos tienen capacidad para seguir alimentando las máquinas incluso en caso de que no reciban electricidad durante un tiempo prudente.

El último problema que ni siquiera las SAI nos pueden protegen es: la corriente estática, un fenómeno extraño del que la mayoría de gente piensa que no afecta a los equipos. Simplemente tocar con la mano la parte metálica de un teclado o de un conductor de una placa puede destruir un equipo completamente. Se trata de una corriente de muy poca intensidad pero muy alta en voltaje, por lo que aunque la persona no sufra ningún daño el ordenador sufre una descarga que puede ser suficiente para destrozar todos sus componentes, desde el disco duro hasta la memoria RAM.

Contra el problema de la corriente estática existen soluciones baratas como por ejemplo: *spray* antiestático y ionizadores antiestáticos. No obstante en la mayoría de situaciones sólo hace falta un poco de precaución de parte del usuario como por ejemplo: no tocar directamente ninguna parte metálica, protegerse si debe hacer operaciones con el hardware, no mantener el entorno excesivamente seco entre otras y así evitar accidentes.

b. Ruido eléctrico.

Dentro del apartado anterior podríamos haber hablado del ruido eléctrico como un problema más relacionado con la electricidad; sin embargo este problema no es una incidencia directa de la corriente en nuestros equipos, sino una incidencia relacionada con la corriente de otras maquinas que pueden afectar el funcionamiento de la nuestra. El ruido eléctrico suele ser generado por motores o por maquinaria pesada, pero también puede serlo por otros ordenadores o por multitud de aparatos.

Para prevenir los problemas que el ruido eléctrico puede causar en nuestros equipos lo más barato es intentar situar el hardware lejos de la maquinaria que puede causar dicho ruido; sino, podemos instalar filtros en las líneas de alimentación que llegan hasta los ordenadores. También es recomendable mantener alejados de los equipos dispositivos emisores de ondas, como teléfonos móviles, transmisores de radio o walkie-talkies; estos elementos puede dañar permanentemente nuestro hardware si

tienen la suficiente potencia de transmisión, o influir directamente en elementos que pueden dañarlo como detectores de incendios o cierto tipo de alarmas.

c. Incendios y humo.

Una causa casi siempre relacionada con la electricidad son los incendios, y con ellos el humo; aunque la causa de un fuego puede ser un desastre natural, lo habitual en muchos entornos es que el mayor peligro de incendio provenga de problemas eléctricos por la sobrecarga de la red debido al gran número de aparatos conectados al tendido eléctrico. Un simple cortocircuito o un equipo que se calienta demasiado pueden convertirse en la causa directa de un incendio en el edificio, o en el departamento de informática, donde se encuentran invertidos millones de dolores en equipamiento.

Un método efectivo contra los incendios son los extintores situados en el techo, que se activan automáticamente al detectar humo o calor. Algunos de ellos, los más antiguos, utilizaban agua para apagar las llamas, lo que provocaba que el hardware no llegara a sufrir los efectos del fuego si los extintores se activaban correctamente, pero quedaba destrozado por el agua expulsada. Visto esté problema, a mitad de los ochenta se comenzaron a utilizar extintores de halón. Este compuesto no conduce electricidad ni deja residuos, por lo que resulta ideal para no dañar los equipos. Sin embargo, también el halón presentaba problemas como: la excesiva contaminación de la atmósfera, y por otro lado puede causar asfixia a las personas a la vez que acaba con el fuego. Por eso se han sustituido los extintores de halón (aunque se siguen utilizando mucho hoy en día) por extintores de dióxido de carbono. Estos son menos contaminantes y ofensivos. De cualquier forma, al igual que el halón el dióxido de carbono no es precisamente sano para los humanos, por lo que antes de activar el extintor es conveniente que todo el mundo abandone la sala; si se trata de sistemas de activación automática suelen avisar antes de expulsar su compuesto mediante un sonido en forma de pito.

Aparte del fuego y el calor generado, en un incendio existe un tercer elemento perjudicial para los equipos: el humo. Este es muy perjudicial para los equipos

especialmente los discos magnéticos y ópticos. Quizás ante un incendio el daño provocado por el humo sea insignificante en comparación con el causado por el fuego y el calor, pero recordemos que puede existir humo sin necesidad de que haya un fuego: por ejemplo, en salas de operaciones donde se fuma.

Aunque muchos no apliquemos esta regla y se fumé demasiado delante de nuestros equipos, sería conveniente no permitir esto; aparte de la suciedad que se deposita en todas las partes de un ordenador, desde el teclado hasta el monitor generada por la ceniza. El humo afecta directamente a todos los componentes; el humo del tabaco es considerado más perjudicial para los equipos y las personas que él de un fuego.

En muchos documentos acerca de la seguridad se insta a los usuarios, administradores, y al personal en general intentar controlar el fuego y salvar el equipo; esto tiene, sus ventajas y sus desventajas. Cuando estamos ante un incendio de pequeñas dimensiones lo común es intentar utilizar un extintor para apagarlo, de forma que lo que podría haber sido una catástrofe sea un simple susto o un pequeño accidente. Sin embargo, cuando las dimensiones de las llamas son considerables lo último que debemos hacer es intentar controlar el fuego porque estaríamos arriesgando nuestras propias vidas para salvar hardware; como sucedía en el caso de inundaciones, no importa el precio de nuestros equipos o el valor de nuestra información: nunca serán tan importantes como nuestra vida. Lo más recomendable en estos casos es evacuar el lugar del incendio y dejar el control en manos de personas especializadas.

d. Temperaturas extremas.

No hace falta ser un especialista para comprender que las temperaturas extremas, ya sea el calor excesivo o un frió intenso, perjudican gravemente a todos los equipos. Es recomendable que los equipos operen entre 10 y 32 grados Celsius, aunque pequeñas variaciones en este rango tampoco han de influir en la mayoría de sistemas.

Para controlar la temperatura ambiente en el entorno de operaciones es recomendable un aire acondicionado, aparato que también influirá positivamente en el rendimiento de los usuarios. Otra condición básica para el correcto funcionamiento de cualquier equipo es que se encuentre correctamente ventilado, sin elementos que obstruyan los ventiladores de la CPU.

La organización física del computador también es decisiva para evitar sobrecalentamientos: si los discos duros, elementos que pueden alcanzar temperaturas considerables, se encuentran excesivamente cerca de la memoria RAM, es muy probable que los módulos acaben quemándose.

4.2.4. Protección de los datos.

La seguridad física también implica una protección a la información de nuestro sistema, tanto la que está almacenada en él como la que se transmite entre diferentes equipos. Aunque en los apartados comentados anteriormente son aplicables a la protección física de los datos ya que si protegemos el hardware también protegemos la información que se almacena o se transmite por él.

hay ciertos aspectos a tener en cuenta a la hora de diseñar una política de seguridad física principalmente porque existen ataques cuyo objetivo no es destruir el medio físico de nuestro sistema, sino simplemente conseguir la información almacenada en dicho medio..

a. Backups.

En este apartado no vamos a hablar de las normas para establecer una política de realización de copias de seguridad correcta, ni tampoco de los mecanismos necesarios para implementarla o de las precauciones que hay que tomar para que todo funcione correctamente; el tema que vamos a tratar en este apartado es la protección física de la información almacenada en backups, esto es, de la protección de los diferentes medios donde residen nuestras copias de seguridad. Hemos de

tener siempre presente que si las copias contienen toda nuestra información tenemos que protegerla igual que protegemos nuestros sistemas.

Un error muy habitual es: almacenar los dispositivos de backup en lugares muy cercanos al departamento de informática o en la mismo departamento; esto, que en principio puede parecer correcto y cómodo cuando necesitemos restaurar los datos, puede convertirse en un problema. Imaginemos que se produce un incendio de grandes dimensiones y todo el edificio queda reducido a cenizas. En este caso extremo tendremos un verdadero problema. Ya que perderíamos nuestros equipos aunque posiblemente el seguro los cubra y todos nuestros datos, tanto los almacenados en los discos como los backups guardados en el mismo edificio.

Como podemos ver, resulta recomendable guardar las copias de seguridad en una zona alejada al departamento de informática, aunque en este caso descentralizamos la seguridad porque tendríamos que proteger el lugar donde almacenamos los backups. Esto en ocasiones puede resultar caro.

Suele ser común etiquetar las cintas donde hacemos copias de seguridad con abundante información sobre su contenido por ejemplo: sistemas de archivos almacenados, día, hora de la realización y sistema al que corresponde; esto tiene una parte positiva y una negativa. Por un lado, recuperar un archivo es rápido: sólo tenemos que ir leyendo las etiquetas hasta encontrar la cinta adecuada. Sin embargo, si nos paramos a pensar, igual que para un administrador es fácil encontrar el backup deseados, también lo es para un intruso que consiga acceso a las cintas, por lo que si el acceso a las mismas no está bien restringido un atacante lo tiene fácil para sustraer una cinta con toda nuestra información.

Los intrusos no necesita saltarse nuestro cortafuego, conseguir una clave del sistema o chantajear a un operador: nosotros mismos le estamos poniendo en bandeja todos nuestros datos. No obstante, ahora nos debemos plantear la duda habitual: si no etiqueto las copias de seguridad, ¿cómo puedo elegir la que debo restaurar en un momento dado? Evidentemente, se necesita cierta información en cada cinta para

poder clasificarlas, pero esa información nunca debe ser algo que le facilite la tarea a un atacante; por ejemplo, se puede diseñar cierta codificación que sólo conozcan las personas responsables de las copias de seguridad, de forma que cada cinta vaya convenientemente etiquetada, pero sin conocer el código. Aunque en un caso extremo el atacante puede llevarse todos nuestros backups para analizarlos uno a uno, siempre es más difícil detectar una carretilla llena de cintas de 8mm que una pequeña unidad guardada en un bolsillo. Y si aún pensamos que alguien puede sustraer todas las copias, simplemente tenemos que realizar backups cifrados y controlar más el acceso al lugar donde las guardamos.

4.2.5. Otros elementos.

En muchas ocasiones los responsables de la seguridad de los sistemas tienen muy presente que la información a proteger se encuentra en los equipos, en las copias de seguridad o circulando por la red, por lo tanto toman medidas para salvaguardar estos medios, pero olvidan que esa información también puede encontrarse en lugares menos obvios, como listados de impresora, facturas telefónicas o la propia documentación de una máquina.

Evidentemente, hay que tomar medidas contra estos problemas. En primer lugar, las impresoras, plotters, faxes, teletipos, o cualquier dispositivo por el que pueda salir información de nuestro sistema ha de estar situado en un lugar de acceso restringido; también es conveniente que sea de acceso restringido el lugar donde los usuarios recogen los documentos que lanzan a estos dispositivos. Sería conveniente que un usuario que recoge una copia se acredite como alguien autorizado a hacerlo, aunque quizás esto puede ser imposible, o al menos muy difícil, en grandes sistemas (imaginemos que en una máquina con cinco mil usuarios obligamos a todo aquél que va a recoger una impresión a identificarse y comprobamos que la identificación es correcta antes de darle su documento con toda seguridad necesitaríamos una persona encargada exclusivamente de este trabajo), siempre es conveniente demostrar cierto grado de interés por el destino de lo que sale por nuestra impresora: sin llegar a realizar un control férreo, si un atacante sabe que el acceso a los

documentos está mínimamente controlado lo pensará dos veces antes de intentar conseguir algo que otro usuario ha impreso.

Elementos que también pueden ser aprovechados por un atacante para comprometer nuestra seguridad son todos aquellos que revelen información de nuestros sistemas o del personal que los utiliza, como: ciertas facturas de teléfono (pueden indicar los números de nuestros módems) o agendas de operadores (revelan los teléfonos de varios usuarios, algo muy provechoso para alguien que intenta efectuar ingeniería social contra ellos). Aunque es conveniente no destruir ni dejar a la vista de todo el mundo esta información, si queremos eliminarla no podemos limitarnos a arrojar documentos a la papelera algo que aunque parezca sacado de películas de espías realmente se utiliza contra todo tipo de entornos. Es recomendable utilizar una trituradora de papel, dispositivo que dificulta muchísimo la reconstrucción y lectura de un documento destruido; por poco dinero podemos conseguir uno de estos aparatos, que suele ser suficiente para acabar con cantidades moderadas de papel.

a. Radiaciones electromagnéticas.

Dentro del apartado 2.2.3 podíamos haber hablado del acceso no autorizado a los datos a través de las radiaciones que el hardware emite; sin embargo, este es un tema que ha cobrado especial importancia en organismos militares a raíz del programa tempest, un término (Transient ElectroMagnetic Pulse Emanation STandard) que identifica una serie de estándares del gobierno estadounidense para limitar las radiaciones eléctricas y electromagnéticas del equipamiento electrónico, desde estaciones de trabajo hasta cables de red, pasando por terminales, mainframes y ratones.

La idea es sencilla: la corriente que circula por un conductor provoca un campo electromagnético alrededor del conductor, el campo varía de la misma forma que lo hace la intensidad de la corriente. Si situamos otro conductor en ese campo, sobre él se induce una señal que también varía proporcionalmente a la intensidad de la corriente inicial; de esta forma, cualquier dispositivo electrónico emite continuamente

radiaciones a través del aire o de conductores, radiaciones que con el equipo adecuado se pueden captar y reproducir remotamente esto implica una amenaza a la seguridad.

Conscientes de este problema en la década de los 50 el gobierno de los Estados Unidos introdujo una serie de estándares para reducir estas radiaciones en los equipos destinados a almacenar, procesar o transmitir información que pudiera comprometer la seguridad nacional. De esta forma, el hardware certificado tempest se suele usar con la información clasificada y confidencial de algunos sistemas gubernamentales para asegurar que el eavesdropping electromagnético no va a afectar la privacidad de los datos.

Casi medio siglo después de las primeras investigaciones sobre amenazas de este tipo, casi todos los países desarrollados y organizaciones militares internacionales tienen programas similares a tempest con el mismo fin: proteger información confidencial. Esta tecnología es reservada para el gobierno y bases militares, restringiendo esta tecnología a organizaciones y a personas particulares. La NRO, National Reconnaissance Office, eliminó en 1992 los estándares tempest para dispositivos de uso doméstico; sin embargo, y como ejemplo de hasta que punto un potencial atacante puede llegar a comprometer la información que circula por una red o que se lee en un monitor, vamos a dar aquí unas nociones generales sobre el problema de las radiaciones electromagnéticas.

Existen numerosos tipos de señales electromagnéticas; sin duda las más peligrosas son las de video y las de transmisión de series, ya que por sus características no es difícil interceptarlas con el equipo adecuado. Otras señales que también son fáciles de captar son: las de enlaces por radiofrecuencia o las de redes basadas en infrarrojos. Estas no presentan tantos problemas ya que desde un principio los diseñadores fueron conscientes de la facilidad de captación y las amenazas a la seguridad que una captura implica; esta inseguridad tan palpable provocó la rápida aparición de mecanismos implementados para dificultar el trabajo de un atacante, como el salto en frecuencias o el espectro disperso, o simplemente el uso de

protocolos cifrados. Este tipo de emisiones quedan fuera del alcance de tempest, pero son cubiertas por otro estándar denominado nonstop, también del Departamento de Defensa estadounidense.

Sin embargo, nadie suele tomar precauciones contra la radiación que emite su monitor, su impresora o el cable de su módem. Y son justamente las radiaciones de este hardware desprotegido las más preocupantes en ciertos entornos, ya que lo único que un atacante necesita para recuperarlas es el equipo adecuado. Dicho equipo puede variar desde esquemas extremadamente simples y baratos pero efectivos, hasta complejos sistemas que en teoría utilizan los servicios de inteligencia de algunos países. La empresa Consumertronics se puede considerar una de las pioneras en la fabrica y venta diversos dispositivos de monitorización.

Pero, ¿cómo podemos protegernos contra el eavesdropping de las radiaciones electromagnéticas de nuestro hardware? Existe un amplio abanico de soluciones, desde simples medidas de prevención hasta las mas complejas para apantallar los equipos. La solución más barata y simple que podemos aplicar es la distancia: las señales que se transmiten por el espacio son atenuadas conforme aumenta la separación de la fuente, por lo que si definimos un perímetro físico de seguridad lo suficientemente grande alrededor de una máquina, será difícil para un atacante interceptar desde lejos nuestras emisiones. No obstante, esto no es aplicable a las señales inducidas a través de conductores, que aunque también se atenúan por la resistencia e inductancia del cableado, la pérdida no es la suficiente para considerar seguro el sistema.

Otra solución consiste en la confusión: cuantas más señales existan en el mismo medio, más difícil será para un atacante filtrar la que está buscando; aunque esta medida no hace imposible la interceptación, sí la dificulta enormemente. Esto se puede conseguir simplemente manteniendo diversas piezas emisoras como por ejemplo: monitores, terminales, cables, etc cercanos entre sí y emitiendo cada uno de ellos información diferente. También existe hardware diseñado explícitamente para crear ruido electromagnético, generalmente a través de señales de radio que

enmascara las radiaciones emitidas por el equipo a proteger; dependiendo de las frecuencias utilizadas, quizás el uso de tales dispositivos pueda ser ilegal: en todos los países el espectro electromagnético está dividido en bandas, cada una de las cuales se asigna a un determinado uso, y en muchas de ellas se necesita una licencia especial para poder transmitir.

La solución más efectiva, y más cara, consiste en el uso de dispositivos certificados que aseguran la mínima emisión, así como de instalaciones que apantallan las radiaciones. En el hardware hay dos aproximaciones principales para prevenir las emisiones: una es la utilización de circuitos especiales que apenas emiten radiación denominados de fuente eliminada, source suppressed, y la otra es la contención de las radiaciones, por ejemplo aumentando la atenuación; generalmente ambas aproximaciones se aplican conjuntamente En cuanto a las instalaciones utilizadas para prevenir el eavesdropping, la idea general es aplicar la contención no sólo a ciertos dispositivos, sino a un edificio o a una sala completa. Quizás la solución más utilizada son las jaulas de Faraday sobre lugares donde se trabaja con información sensible; se trata de separar el espacio en dos zonas electro magnéticamente aisladas por ejemplo, una sala y el resto del espacio de forma que fuera de una zona en donde no se pudieran captar las emisiones que se producen en su interior. Para implementar esta solución se utilizan materiales especiales, como algunas clases de cristal, o simplemente un recubrimiento conductor conectado a tierra.

Antes de finalizar este punto quizás es recomendable volver a insistir en que todos los problemas y soluciones derivados de las radiaciones electromagnéticas no son aplicables a los entornos o empresas normales, sino que están pensados para lugares donde se trabaja con información altamente confidencial, como ciertas empresas u organismos militares o de inteligencia. Aquí simplemente se han presentado como una introducción para mostrar hasta donde puede llegar la preocupación por la seguridad en esos lugares. La radiación electromagnética no es un riesgo importante en la mayoría de organizaciones ya que suele tratarse de un ataque costoso en tiempo y dinero, de forma que un atacante suele tener muchas otras puertas para intentar comprometer el sistema de una forma más fácil.

CAPITULO 5. IMPLEMENTACIÓN DE SEGURIDAD ANTIVIRUS

La seguridad antivirus en uno de los componentes mas importantes que forma parte de la seguridad de redes y es un elemento imprescindible para la estrategia de seguridad “defensa en profundidad” ya que aporta una de las líneas de defensa mas completa al prevenir una de las amenazas mas frecuente y dañina a las que una red corporativa esta expuesta.

Puntos clave:

- Conocer conceptos básicos sobre virus, funcionamiento, clasificación, modos de operación y síntomas mas comunes.

- Mencionar que es un software antivirus, funciones y técnicas de detección.

- Describir las diferentes características que deben cumplir los software antivirus

- Listar los diferentes software antivirus disponibles en el mercado

- Mencionar políticas antivirus

- Definir estrategias antivirus

- Conocer conceptos básicos sobre spyware, métodos y señales de infección, así también como prevenirlos y removerlos.

Los virus informáticos son uno de los principales riesgos de seguridad para las redes internas corporativas, ya sea que se este hablando de un usuario hogareño que utiliza su máquina para trabajar y conectarse a Internet o una organización con un sistema informático importante que debe mantener bajo constante vigilancia para evitar pérdidas causadas por los virus.

Un virus se valdrá de cualquier técnica conocida o poco conocida para lograr su cometido. Así, se encontraran virus muy simples que sólo se dedican a presentar mensajes en pantalla y algún otro mucho más complejo que intentan ocultar su presencia y atacar en el momento justo.

A lo largo del presente capitulo se hará referencia a qué es exactamente un virus, cómo trabaja, algunos tipos de virus y también cómo combatirlos. Se propondrá dar una visión general de los tipos de virus existentes para poder enfocarse más en cómo proteger una red corporativa de estos atacantes y cómo erradicarlos una vez que logran penetrar.

5.1 CONCEPTOS BÁSICOS SOBRE VIRUS INFORMÁTICOS

5.1.1 ¿Qué es un virus informático?

Un virus informático es un programa de computadora que tiene la capacidad de causar daño y su característica más relevante es que puede replicarse a sí mismo y propagarse a otras computadoras. Infecta "entidades ejecutables": cualquier archivo o sector de las unidades de almacenamiento que contenga códigos de instrucción que el procesador vaya a ejecutar.

Un virus es un programa que automatiza un ataque en una computadora o red. Este tiene típicamente intenciones maliciosas, van desde desestabilización de accesos hacia poder de computo y robo de datos con el fin de utilizar la computadora infectada para atacar otras computadoras.

Un virus tiene tres características primarias:

- **Es dañino**. Un virus informático siempre causa daños en el sistema que infecta, pero vale aclarar que el hacer daño no significa que vaya a romper algo. El daño puede ser implícito cuando lo que se busca es destruir o alterar información o pueden ser situaciones con efectos negativos para la computadora, como consumo de memoria principal, tiempo de procesador y disminución del desempeño.
- **Es autor reproductor**. La característica más importante de este tipo de programas es la de crear copias de sí mismo, cosa que ningún otro programa convencional hace. Imagínense que si todos tuvieran esta capacidad podríamos instalar un procesador de textos y un par de días más tarde tendríamos tres de ellos o más. Consideramos ésta como una característica propia de virus porque los programas convencionales pueden causar daño, aunque sea accidental, sobrescribiendo algunas librerías y pueden estar ocultos a la vista del usuario, por ejemplo: un programita que se encargue de legitimar las copias de software que se instalan.
- **Es subrepticio**. Esto significa que utilizará varias técnicas para evitar que el usuario se de cuenta de su presencia. La primera medida es tener un tamaño reducido para poder disimularse a primera vista. Puede llegar a manipular el resultado de una petición al sistema operativo de mostrar el tamaño del archivo e incluso todos sus atributos.

La verdadera peligrosidad de un virus no está dada por su arsenal de instrucciones maléficas, sino por lo crítico del sistema que está infectando. Tomemos como ejemplo un virus del tipo conejo. Si este infectara una computadora hogareña la máquina dejara de funcionar (congelada), pudiendo luego reiniciarla con un disquete de arranque limpio y con un antivirus para eliminar el virus. Si afectara a un servidor de una organización, posiblemente el sistema informático de la organización dejaría de funcionar por algún tiempo significando una pérdida de horas máquina y de dinero. Pero si este virus infectara una máquina industrial como una grúa robótica o

algún aparato utilizado en medicina como una máquina de rayos láser para operar, los costos serían muy altos y posiblemente se perderían vidas humanas. ¿Qué pasaría si se alteraran los registros médicos de una persona de forma que se mostrara un tipo de sangre o factor RH diferente? El paciente podría morir. ¿Qué pasaría si el dígito 4 millonésimos en los cálculos para el aterrizaje de una misión espacial se alteraran en un factor del 0.001 por 100? Los astronautas morirían.

Los virus informáticos no pueden causar un daño directo sobre el hardware. No existen instrucciones que derritan la unidad de disco rígido o que hagan estallar el cañón de un monitor. En su defecto, un virus puede hacer ejecutar operaciones que reduzcan la vida útil de los dispositivos. Por ejemplo: hacer que la placa de sonido envíe señales de frecuencias variadas con un volumen muy alto para averiar los parlantes, hacer que la impresora desplace el cabezal de un lado a otro o que lo golpee contra uno de los lados, hacer que las unidades de almacenamiento muevan a gran velocidad las cabezas de Lectura/Escritura para que se desgasten. Todo este tipo de cosas son posibles aunque muy poco probables y por lo general los virus prefieren atacar los archivos y no meterse con la parte física.

5.1.2 ¿Quién los hace?

En primer lugar se debe decir que los virus informáticos están hechos por personas con conocimientos de programación pero que no son necesariamente genios de las computadoras. Tienen conocimientos de lenguaje de programación como Visual Basic, Visual Basic Script, Lenguaje C/C++, etc y de cómo funciona internamente la computadora. De hecho resulta bastante más difícil hacer un programa "en regla" como sería un sistema de facturación en donde hay que tener muchísimas más cosas en cuenta que en un simple virus que aunque esté mal programado sería suficiente para molestar al usuario.

En un principio estos programas eran diseñados casi exclusivamente por los hackers y crackers que tenían su auge en los Estados Unidos y que hacían temblar a las compañías con solo pensar en sus actividades. Tal vez esas personas lo hacían con

la necesidad de demostrar su creatividad y su dominio de las computadoras, por diversión o como una forma de manifestar su repudio a la sociedad que los oprimía. Hoy en día, resultan un buen medio para el sabotaje corporativo, espionaje industrial y daños a material de una empresa en particular.

5.2 FUNCIONAMIENTO DE LOS VIRUS

Los virus informáticos están hechos en lenguajes de programación como Visual Basic, Visual Basic Script, Lenguaje C/C++, etc, los cuales son lenguajes de programación de alto nivel. Las instrucciones compiladas por estos lenguajes trabajan directamente sobre el hardware, esto significa que no es necesario ningún software intermedio, según el esquema de capas entre usuario y hardware

Sabiendo esto, el virus puede tener control total de la máquina al igual que lo hace el sistema operativo si logra cargarse antes que nadie. La necesidad de tener que "asociarse" a una entidad ejecutable viene de que, como cualquier otro programa de computadora, necesita ser ejecutado y teniendo en cuenta que ningún usuario en su sano juicio lo hará, se vale de otros métodos furtivos. Ahora que se ha marcado la importancia para un virus el ser ejecutado, se puede decir que un virus puede encontrarse en una computadora sin haber infectado realmente algo. Es el caso de personas que pueden coleccionar virus en archivos comprimidos o encriptados.

Normalmente este tipo de programas se adhiere a alguna entidad ejecutable que le facilitará la subida a memoria principal y la posterior ejecución (métodos de infección). Como entidades ejecutables se pueden reconocer a los sectores de arranque de los discos de almacenamiento magnéticos, ópticos o magneto-ópticos (MBR, BR), los archivos ejecutables de DOS (.exe, .com, entre otros), las librerías o módulos de programas (.dll, .lib, .ovl, .bin, .ovr). Los sectores de arranque son fundamentales para garantizar que el virus será cargado cada vez que se encienda la computadora.

Según la secuencia de booteo de las computadoras, el microprocesador tiene configurado de fábrica la dirección de donde puede obtener la primer instrucción a ejecutar. Esta dirección apunta a una celda de la memoria ROM donde se encuentra la subrutina POST (Power On Self Test), encargada de varias verificaciones y de comparar el registro de la memoria CMOS con el hardware instalado (función checksum). En este punto sería imposible que el virus logre cargarse ya que la memoria ROM viene grabada de fábrica y no puede modificarse (hoy en día las memorias Flash-ROM podrían contradecir esto último).

Luego, el POST pasa el control a otra subrutina de la ROM BIOS llamada "bootstrap ROM" que copia el MBR (Master Boot Record) en memoria RAM. El MBR contiene la información de la tabla de particiones, para conocer las delimitaciones de cada partición, su tamaño y cuál es la partición activa desde donde se cargará el SO. Puede observarse que en este punto el procesador empieza a ejecutar de la memoria RAM, dando la posibilidad a que un virus tome partida. Hasta acá el SO todavía no fue cargado y en consecuencia tampoco el antivirus. El accionar típico del virus sería copiar el MBR en un sector alternativo y tomar su posición. Así, cada vez que se inicie el sistema el virus logrará cargarse antes que el SO y luego, respetando su deseo por permanecer oculto hará ejecutar las instrucciones del MBR.

Con la información del MBR se sabe qué partición es la activa y en que sector se encuentra su sector de booteo (boot record o BR). El BR contiene una subrutina que se ocupará de cargar los archivos de arranque del SO. Los demás pasos de la carga del SO son irrelevantes, pero es importante recordar que el SO es el último en cargarse en la secuencia de booteo antes de que el usuario pueda introducir comandos en el shell. El antivirus es cargado por los archivos de configuración del SO personalizables por el usuario.

Cuando un virus infecta un archivo ejecutable .EXE, por ejemplo, intenta rastrear en el código los puntos de entrada y salida del programa. El primer punto señalado es en donde, dentro del archivo, se iniciará la ejecución de instrucciones. El segundo punto resulta ser lo opuesto. Cuando un virus localiza ambos puntos escribe su

propio código antes de cada uno. Según el tipo de virus, este código cargará el virus en memoria –si es que no lo estaba- y apuntará a esa zona infectada con el virus. A partir de ahí el programa de virus determinará cuáles son las acciones a seguir: puede continuar infectando archivos que sean cargados en memoria, ocultarse si es que detecta la presencia de un antivirus o ejecutar el contenido de su módulo de ataque. El virus puede infectar también las copias de los archivos cargados en memoria que están en la unidad de almacenamiento. Así se asegura que ante un eventual apagado de la computadora su código igualmente se encuentra en los archivos de la unidad.

Es importante comprender que la computadora no estará infectada hasta que se ejecute algo infectado previamente con el virus. Esto se vera con un ejemplo sencillo: cuando se baja del Internet un archivo comprimido (con la extensión .ZIP según el uso popular) aun sabiendo que es un programa de prueba que se quisiera instalar. Lo que no se sabe es que uno de los archivos dentro del .ZIP es un virus informático y lo peor de todo es que viene adherido al archivo Install.exe. Al momento de descomprimir el contenido, el virus todavía no fue ejecutado (ya que la información dentro del .ZIP no puede ser reconocida como instrucciones por el procesador). Luego identificamos el archivo Install.exe como el necesario para instalar el programa y lo ejecutamos. Recién en este momento el virus se cargará en memoria y pasará a hacer las cosas para lo que fue programado.

El ejemplo anterior es un modo muy básico de infección. Pero existen otros tantos tipos de virus que son mucho más sofisticados y no podrá ser reconocida su presencia con mucha facilidad.

Según sus características un virus puede contener tres módulos principales: el módulo de ataque, el módulo de reproducción y el módulo de defensa.

- **Módulo de reproducción**. Es el encargado de manejar las rutinas para infectar entidades ejecutables que asegurarán la subsistencia del virus. Cuando toma el control del sistema puede infectar otras entidades

ejecutables. Cuando estas entidades sean trasladadas a otras computadoras se asegura la dispersión del virus.

- **Módulo de ataque**. Es el módulo que contiene las rutinas de daño adicional o implícito. El módulo puede ser activado por distintos eventos del sistema: una fecha, hora, el encontrar un archivo específico (COMMAND.COM), el encontrar un sector específico (MBR), una determinada cantidad de booteos desde que ingreso al sistema o cualquier otra cosa a la que el programador quisiera atacar.
- **Módulo de defensa**. Su principal objetivo es proteger el cuerpo del virus. Incluirá rutinas que disminuyan los síntomas que delaten su presencia e intentarán que el virus permanezca invisible a los ojos del usuario y del antivirus. Las técnicas incluidas en este módulo hoy en día resultan ser muy sofisticadas logrando dar información falsa al SO -y en consecuencia al usuario- y localizándose en lugares poco comunes para el registro de los antivirus como la memoria Flash-Rom.

5.3 ALGUNOS MÉTODOS DE INFECCIÓN

A continuación se describen algunos de los métodos de infección existentes:

- **Añadidura o empalme**. Por este método el código del virus se agrega al final del archivo ejecutable a infectar, modificando las estructuras de arranque del archivo anfitrión de manera que el control del programa pase primero al virus cuando se quiera ejecutar el archivo. Este cambio de secuencia permite al virus realizar sus tareas específicas y luego pasar el control al programa para que este se ejecute normalmente. La principal desventaja de este método es que el tamaño del archivo infectado es mayor al original, lo que permite una fácil detección.
- **Inserción**. Los virus que utilizan el método de inserción buscan alojarse en zonas de código no utilizadas o en segmentos de datos dentro de los archivos que contagian, de esta manera la longitud total del archivo infectado no varía. Este método, parecido al de empalme, exige mayores técnicas de

programación de los virus para poder detectar las zonas posibles de contagio dentro de un ejecutable, por lo que generalmente no es muy utilizada por los programadores de virus informáticos.

- **Reorientación**. Este método es una variante interesante del anterior. Bajo este esquema se introducen centrales virales (los códigos principales del virus) en zonas físicas del disco rígido marcadas como defectuosas o en archivos ocultos del sistema. Estos códigos virales, al ejecutarse, implantan pequeños trozos de código en los archivos ejecutables que infectan, que luego actúan como llamadores de las centrales virales. La principal ventaja de este método es que el cuerpo del virus, al no estar agregado en el archivo infectado sino en otro sitio oculto, puede tener un tamaño bastante grande, aumentando así su funcionalidad. La desventaja más fuerte es que la eliminación de este tipo de infecciones es bastante sencilla. Basta con borrar archivos ocultos sospechosos o reescribir las zonas del disco marcadas como defectuosas.
- **Polimorfismo**. Este es el método más avanzado de contagio logrado por los programadores de virus. La técnica básica usada es la de inserción del código viral en un archivo ejecutable, pero para evitar el aumento de tamaño del archivo infectado, el virus compacta parte de su código y del código del archivo anfitrión de manera que la suma de ambos sea igual al tamaño original del archivo. Al ejecutar el programa infectado actúa primero el código del virus descompreso en memoria las porciones previamente compactadas. Una variante mejorada de esta técnica permite a los virus usar métodos de encriptación dinámicos para disfrazar el código del virus y evitar ser detectados por los antivirus.
- **Sustitución**. El método de sustitución, usado con variantes por los Caballos de Troya, es quizás el método más primitivo. Consiste en sustituir el código completo del archivo original por el código del virus. Al ejecutar el programa infectado el único que actúa es el virus, que cumple con sus tareas de contagiar otros archivos y luego termina la ejecución del programa reportando algún tipo de error. Esta técnica tiene sus ventajas, ya que en cada infección

se eliminan archivos de programas válidos, los cuales son reemplazados por nuevas copias del virus.

- **Tunneling**. Es una técnica usada por programadores de virus y antivirus para evitar todas las rutinas al servicio de una interrupción y tener así un control directo sobre esta. Requiere una programación compleja, hay que colocar el procesador en modo kernel. En este modo de funcionamiento, tras ejecutarse cada instrucción se produce la INT 1. Se coloca una ISR (Interrupt Service Routine) para dicha interrupción y se ejecutan instrucciones comprobando cada vez si se ha llegado a donde se quería hasta recorrer toda la cadena de ISRs que halla colocando el parche al final de la cadena.

Los virus utilizan el tunneling para protegerse de los módulos residentes de los antivirus que monitorean todo lo que sucede en la máquina para interceptar todas las actividades "típicas" de los virus.

Para entender como funciona esta técnica basta saber como trabaja este tipo de antivirus. El módulo residente queda colgado de todas las interrupciones usualmente usadas por los virus (INT 21, INT 13, a veces INT 25 Y 26) y entonces cuando el virus intenta llamar a INT 21, por ejemplo, para abrir un ejecutable para lectura / escritura (y luego infectarlo), el antivirus emite una alerta, pues los ejecutables no son normalmente abiertos, ni menos para escritura. Y así con todas las llamadas típicas de los virus.

En cambio, cuando se hace una llamada común y corriente, el antivirus no le da mayor importancia y la deja pasar, llamando a la INT 21 original. Un virus con tunneling, entonces, antes de llamar a ninguna función ni hacer nada, intenta obtener la dirección absoluta de esta INT 21 original, que está en alguna parte de la memoria del antivirus residente. Una vez que obtiene esta dirección, accede al MS-DOS por medio de el, sin llamar al antivirus.

Ejemplos de cómo un virus puede ser contraído:

- A través de archivos adjuntos en los correos electrónicos y redes de intercambio de archivos P2P.
- Al abrir un correo electrónico vía HTML.
- Mediante la transferencia física desde una computadora infectada a través de un medio de almacenamiento (disco flexible, CD, memoria flash, etc).
- Mediante el uso de software infectado, entre los que se tienen: software comercial, gratis, libre distribución o discos de datos.
- Mediante el acceso por parte del usuario a sitios web con contenido sexual ya se intencionalmente o por equivocación.

Ejemplos de cómo un virus se propaga:

- Aprovechando las fallas de software.
- Utilizando errores de programación (bugs) en protocolos comunes como el SSL (Secure Socket Layer).
- Aprovechando las debilidades del protocolo TCP/IP
- Aprovechando el comportamiento humano
- Analizando constantemente sistemas conectados a la red, buscando y aprovechando las vulnerabilidades conocidas.

5.4. CLASIFICACIÓN DE LOS VIRUS

La clasificación correcta de los virus siempre resulta variada según a quien se le pregunte. Se pueden agrupar por la entidad que infectan (sectores de arranque o archivos ejecutables), por su grado de dispersión a nivel mundial, por su comportamiento, por su agresividad, por sus técnicas de ataque o por como se oculta, etc .En algunos casos un virus puede incluirse en más de un tipo (un multipartito resulta ser sigiloso). La clasificación de los virus se muestra a continuación:

- Caballos de Troya

- Camaleones
- Virus polimorfos o mutantes
- Virus sigiloso o stealth
- Virus lentos
- Retro-virus o Virus antivirus
- Virus multipartitos
- Virus voraces
- Bombas de tiempo
- Conejo
- Macro-virus
- Worm
- Virus Falsos o Hoaxes

5.5. DETERMINAR SI EXISTE INFECCIÓN

Realmente nadie puede determinar a ciencia cierta qué síntomas muestra el sistema cuando está infectado ya que los virus son muy variados y sus formas de comportamiento también, a esto se suma que en la actualidad los virus bien programados son mucho más sofisticados que antes y reconocer la presencia de un virus con un simple vistazo no es una habilidad que muchos puedan ostentar.

Podemos mencionar algunos indicios que delatarían la presencia de un virus pero la lista no es definitiva:

- *Los comandos o acciones que se hacen ejecutar por la computadora aparentan ser más lentos*. Esto es debido a que hay un programita extra que no está en nuestros cálculos y que trabaja sobre cada una de las cosas que nosotros hacemos. De todas formas resulta un poco improbable ya que el tamaño de los virus, por lo general, no da lugar a que realicen extensas ejecuciones, descontando obviamente la lentitud de cualquier dispositivo periférico.

- Las aplicaciones que ya de por sí son un tanto pesadas en cargarse ahora resultan aún más pesadas.
- Dispositivos como disco duro o el drive del disco flexible son leídos repentinamente sin causa o motivo. Esto puede pasar cuando un virus intenta propagarse a un disquete, por ejemplo.
- Los *archivos* se incrementan levemente en tamaño. Puede ser a causa de un virus que infecta a esos archivos agregando su código al código ejecutable del archivo. En la actualidad resulta más difícil detectar un virus de estos ya que las técnicas stealth permiten que el virus manipule el tamaño de archivo que el usuario termina viendo en la pantalla. El resultado es que el usuario termina viendo el tamaño que tenía el archivo antes de ser infectado en vez del tamaño real actual.
- Programas o *procesos* en *memoria* que son desconocidos. Para un usuario experimentado resultaría extraño ver en memoria un proceso que él no autorizó a que sea cargado. Los sistemas operativos poseen distintos comandos o programas que permiten ver el estado de la memoria y poder determinar que programas se encuentran cargados en ese momento, entre otras cosas como la dirección en donde están localizados, el tamaño que ocupan, etc.

Existen otras manifestaciones que muchos confunden con síntomas cuando en realidad no lo son. Gráficos poco comunes que aparecen en la pantalla, mensajes nunca antes vistos, letras que se caen y rebotan en el fondo de la pantalla y todo otro tipo de cosas similar no son más que el accionar propio del virus. Los virus fueron programados para ese tipo de cosas por más ridículas que parezcan para algunos y no son consecuencias secundarias en el sistema debido a que exista un virus.

5.6. SÍNTOMAS MÁS COMUNES DE VIRUS

Incluso el mejor software antivirus puede fallar a la hora de detectar un virus. La educación del personal sobre cuáles son posibles síntomas de virus informáticos puede ser la diferencia entre un simple dolor de cabeza y un gran problema.

A continuación se presentan algunos síntomas:

- Los programas comienzan a ocupar más espacio de lo habitual.
- Aparecen o desaparecen archivos.
- Cambia el tamaño de un *programa* o un objeto.
- Aparecen mensajes u objetos extraños en la pantalla.
- El disco trabaja más de lo necesario.
- Los objetos que se encuentran en la pantalla aparecen ligeramente distorsionados.
- La cantidad de espacio libre del disco disminuye sin ningún tipo de explicación,
- Se modifican sin razón aparente el nombre de los ficheros.
- No se puede acceder al disco duro

5.7. CÓMO PROCEDER ANTE UNA INFECCIÓN

Cuando el antivirus logra confirmar la presencia de un virus, lo primero que siente el usuario es pánico. Luego pensará qué hacer y se dará cuenta que no tiene idea cómo enfrentarse a un virus informático. Educar a los usuarios sobre estas cuestiones es tan importante como mantenerlos actualizados de los últimos virus que aparecen.

En este capitulo no se intentara describir paso a paso la solución cuando se tiene un antivirus actualizado que posiblemente haga todo por nosotros y solo nos solicita que tomemos una decisión. En su lugar, el enfoque será visto desde la perspectiva del antivirus para determinar qué se debe hacer contra un virus una vez que ha reconocido un accionar viral en el sistema. En algunas oportunidades no se tendrá otra salida más que utilizar una extracción manual realizada por el usuario mismo. Es muy común este tipo de cosas con los virus de última generación ya que no les dan tiempo a los fabricantes de antivirus a actualizar sus definiciones de virus.

5.8. PROGRAMAS ANTIVIRUS

Los riesgos que infunden los virus hoy en día obligaron a que empresas enteras se dediquen a buscar la forma de crear programas con fines comerciales que logren combatir con cierta eficacia los virus que ataquen los sistemas informáticos. Este software es conocido con el nombre de programas *antivirus* y posee algunas características interesantes para poder cumplir su trabajo.

Como ya se menciono con anterioridad una de las características fundamentales de un virus es propagarse infectando determinados objetos según fue programado. En el caso de los que infectan archivos, el virus debe poseer algún método para no infectar los archivos con su propio código –para evitar autodestruirse, en otras palabras-, así es que dejan una marca o firma que los identifica de los demás programas o virus.

Para la mayoría de los virus esta marca representa una cadena de caracteres que "inyectan" en el archivo infectado. Los virus más complejos como los polimorfos poseen una firma algorítmica que modificará el cuerpo del mismo con cada infección. Cada vez que estos virus infecten un archivo, mutará su forma y dificultará bastante más las cosas para el software de detección de virus.

El software antivirus es un programa más de computadora y como tal debe ser adecuado para nuestro sistema y debe estar correctamente configurado según los dispositivos de hardware que estén instalados en el sistema. Si el usuario trabaja en un lugar que posee conexión a redes es necesario tener un programa antivirus que tenga la capacidad de detectar virus de redes. Los antivirus reducen sensiblemente los riesgos de infección pero cabe reconocer que no serán eficaces el cien por ciento de las veces y su utilización debería estar acompañada con otras formas de prevención.

La función primordial de un programa de estos es detectar la presencia de un posible virus para luego poder tomar las medidas necesarias. El hecho de poder erradicarlo podría considerarse como una tarea secundaria ya que con el primer paso habremos logrado frenar el avance del virus, cometido suficiente para evitar mayores daños.

Antes de profundizar en el tema del software antivirus es importante que conocer la diferencia entre *detectar* un virus e *identificar* un virus. El detectar un virus es reconocer la presencia de un accionar viral en el sistema de acuerdo a las características de los tipos de virus. Identificar un virus es poder reconocer qué virus es de entre una larga lista de otros virus cargados en la base de datos. Al identificarlo se sabrá exactamente qué es lo que hace, haciendo inminente su eliminación.

De los dos métodos mencionados anteriormente es importante que un antivirus sea más fuerte en el tema de la detección, ya que con este método podremos encontrar virus todavía no conocidos (de reciente aparición) y que seguramente no estarán registrados en nuestra base de datos debido a que su tiempo de dispersión no es suficiente como para que hayan sido analizados por un grupo de expertos de la empresa del antivirus.

5.8.1. Identificación

Identificar un virus supone, primero, lograr su detección y luego poder determinar de qué virus se trata exactamente. A esta técnica se la conoce con el nombre de *scanning* o *escaneo*. Esta técnica es muy sencilla de entender. El programa antivirus posee una base de datos con ciertos *strings* propios de cada virus. Estos strings no son más que las firmas o sea cadenas de caracteres que el scanner del antivirus utilizará como huella digital para identificar de qué virus se trata. El scanner comienza a revisar uno por uno el código de los archivos almacenados intentando encontrar alguno de estos fragmentos representativos de los virus que tiene registrados. Con cada una de las verificaciones no se revisa la base de datos completa ya que resultaría bastante trabajoso y en una pérdida de tiempo considerable, aunque de hecho el hacer un escaneo de nuestra unidad de disco

rígido lleva algún tiempo. Entonces, cada antivirus utilizará diferentes técnicas algorítmicas para agilizar un poco este paso de comparar el código contra su base de datos.

Hoy en día la producción de virus se ve masificada e Internet colabora enormemente en la dispersión de virus de muchos tipos, incluyendo los "virus caseros". Muchos de estos virus son creados por usuarios inexpertos con pocos conocimientos de programación y, en muchos casos, por simples usuarios que bajan de Internet programas que crean virus genéricos. Ante tantos "desarrolladores" al servicio de la producción de virus la técnica de scanning se ve altamente superada. Las empresas antivirus están constantemente trabajando en la búsqueda y documentación de cada nuevo virus que aparece. Muchas de estas empresas actualizan sus bases de datos todos los meses, otras lo hacen quincenalmente, y algunas pocas llegan a hacerlo todas las semanas (cosa más que importante para empresas que necesitan una alta protección en este campo o para usuarios fanáticos de obtener lo último en seguridad y protección).

La debilidad de la técnica de scanning es inherente al modelo. Esto es debido a que un virus debería alcanzar una dispersión adecuada para que algún usuario lo capture y lo envíe a un grupo de especialistas en virus que luego se encargarán de determinar que parte del código será representativa para ese virus y finalmente lo incluirán en la base de datos del antivirus. Todo este proceso puede llevar varias semanas, tiempo suficiente para que un virus eficaz haga de las suyas. En la actualidad, Internet proporciona el canal de bajada de las definiciones antivirus que nos permitirán identificar decenas de miles de virus que andan acechando. Estas decenas de miles de virus, como se menciono anteriormente, también influirán en el tamaño de la base de datos. Como ejemplo concreto podemos mencionar que la base de datos de Norton Antivirus de Symantec Corp. pesa alrededor de 10MB y es actualizada cada quince o veinte días.

La técnica de scanning no resulta ser la solución definitiva, ni tampoco la más eficiente, pero continúa siendo la más utilizada debido a que permite identificar con

cierta rapidez los virus más conocidos, que en definitiva son los que lograron adquirir mayor dispersión.

5.8.2. Técnicas de detección

Teniendo en cuenta los puntos débiles de la técnica de scanning surgió la necesidad de incorporar otros métodos que complementaran al primero. Como ya se mencionó la detección consiste en reconocer el accionar de un virus por los conocimientos sobre comportamiento que se tienen sobre ellos, sin importar demasiado su identificación exacta. Este otro método buscará código que intente modificar la información de áreas sensibles del sistema sobre las cuales el usuario convencional no tiene control y a veces ni siquiera tiene conocimiento, como el master boot record, el boot sector, la FAT, entre las más conocidas.

Otra forma de detección que se puede mencionar adopta, más bien, una posición de vigilancia constante y pasiva. Esta, monitorea cada una de las actividades que se realizan intentando determinar cuándo una de éstas intenta modificar sectores críticos de las unidades de almacenamiento, entre otros. A esta técnica se la conoce como *chequear la integridad*.

5.8.3. Análisis heurístico

La técnica de detección más común es la de análisis heurístico. Consiste en buscar en el código de cada uno de los archivos cualquier instrucción que sea potencialmente dañina, acción típica de los virus informáticos. Es una solución interesante tanto para virus conocidos como para los que no lo son. El inconveniente es que muchas veces se nos presentarán falsas alarmas, cosas que el scanner heurístico considera peligrosas y que en realidad no lo son tanto. Por ejemplo: tal vez el programa revise el código del comando DEL (usado para borrar archivos) de MS-DOS y determine que puede ser un virus, cosa que en la realidad resulta bastante improbable. Este tipo de cosas hace que el usuario deba tener algunos

conocimientos precisos sobre su sistema, con el fin de poder distinguir entre una falsa alarma y una detección real.

5.8.4. Eliminación

La eliminación de un virus implica extraer el código del archivo infectado y reparar de la mejor manera el daño causado en este. A pesar de que los programas antivirus pueden detectar miles de virus, no siempre pueden erradicar la misma cantidad, por lo general pueden quitar los virus conocidos y más difundidos de los cuales pudo realizarse un análisis profundo de su código y de su comportamiento. Resulta lógico entonces que muchos antivirus tengan problemas en la detección y erradicación de virus de comportamiento complejo, como el caso de los polimorfos, que utilizan métodos de encriptación para mantenerse indetectables. En muchos casos el procedimiento de eliminación puede resultar peligroso para la integridad de los archivos infectados, ya que si el virus no está debidamente identificado las técnicas de erradicación no serán las adecuadas para el tipo de virus.

Hoy en día los antivirus más populares están muy avanzados pero cabe la posibilidad de que este tipo de errores se de en programas más viejos. Para muchos el procedimiento correcto sería eliminar completamente el archivo y restaurarlo de la copia de respaldo. Si en vez de archivos la infección se realizó en algún sector crítico de la unidad de disco rígido la solución es simple, aunque no menos riesgosa. Hay muchas personas que recomiendan reparticionar la unidad y reformatearla para asegurarse de la desaparición total del virus, cosa que resultaría poco operativa y fatal para la información del sistema. Como alternativa a esto existe para el sistema operativo MS-DOS / Windows una opción no documentada del comando FDISK que resuelve todo en cuestión de segundos. El parámetro /MBR se encarga de restaurar el registro maestro de booteo (lugar donde suelen situarse los virus) impidiendo así que este vuelva a cargarse en el inicio del sistema. Vale aclarar que cualquier dato que haya en ese sector será sobrescrito y puede afectar mucho a sistemas que tengan la opción de bootear con diferentes sistemas operativos. Muchos de estos programas que permiten hacer la elección del sistema operativo se sitúan en esta

área y por consiguiente su código será eliminado cuando se usa el parámetro mencionado.

5.8.5. Comprobación de integridad

Como ya se había anticipado con anterioridad los comprobadores de integridad verifican que algunos sectores sensibles del sistema no sean alterados sin el consentimiento del usuario. Estas comprobaciones pueden aplicarse tanto a archivos como al sector de arranque de las unidades de almacenamiento.
Para poder realizar las comprobaciones el antivirus, primero, debe tener una imagen del contenido de la unidad de almacenamiento desinfectada con la cual poder hacer después las comparaciones. Se crea entonces un registro con las características de los archivos, como puede ser su nombre, tamaño, fecha de creación o modificación y, lo más importante para el caso, el checksum, que es aplicar un algoritmo al código del archivo para obtener un valor que será único según su contenido (algo muy similar a lo que hace la función hash en los mensajes). Si un virus inyectara parte de su código en el archivo la nueva comprobación del checksum sería distinta a la que se guardó en el registro y el antivirus alertaría de la modificación. En el caso del sector de booteo el registro puede ser algo diferente. Como existe un MBR por unidad física y un BR por cada unidad lógica, algunos antivirus pueden guardarse directamente una copia de cada uno de ellos en un archivo y luego compararlos contra los que se encuentran en las posiciones originales.

Una vez que el antivirus conforma un registro de cada uno de los archivos en la unidad podrá realizar las comprobaciones de integridad. Cuando el comprobador es puesto en funcionamiento cada uno de los archivos serán escaneados. Nuevamente se aplica la función checksum y se obtiene un valor que es comparado contra el que se guardó en el registro. Si ambos valores son iguales el archivo no sufrió modificaciones durante el período comprendido entre el registro de cheksum antiguo y la comprobación reciente. Por el otro lado, si los valores checksum no concuerdan significa que el archivo fue alterado y en ciertos casos el antivirus pregunta al usuario si quiere restaurar las modificaciones. Lo más indicado en estos casos sería que un

usuario con conocimientos sobre su sistema avale que se trata realmente de una modificación no autorizada y por lo tanto atribuible a un virus, por lo hay que eliminar el archivo y restaurarlo desde la copia de respaldo.

La comprobación de integridad en los sectores de booteo no es muy diferente. El comprobador verificará que la copia que está en uso sea igual a la que fue guardada con anterioridad. Si se detectara una modificación en cualquiera de estos sectores, se preguntará al usuario por la posibilidad de reconstruirlos utilizando las copias guardadas. Teniendo en cuenta que este sector en especial es un punto muy vulnerable a la entrada de los virus multipartitos, los antivirus verifican constantemente que no se hagan modificaciones. Cuando se detecta una operación de escritura en uno de los sectores de arranque, el programa toma cartas en el asunto mostrando en pantalla un mensaje para el usuario indicándole sobre qué es lo que está por suceder. Por lo general el programa antivirus ofrece algunas opciones sobre como proceder, como evitar la modificación, dejarla continuar, congelar el sistema o no tomar ninguna medida (cancelar).

Para que esta técnica sea efectiva cada uno de los archivos deberá poseer su entrada correspondiente en el registro de comprobaciones. Si nuevos programas se están instalando o estamos bajando algunos archivos desde Internet, o algún otro archivo ingresa por cualquier otro dispositivo de entrada, después sería razonable que registremos el checksum con el comprobador del antivirus. Incluso, algunos de estos programas atienden con mucha atención a lo que el comprobador de integridad determine y no dejarán que ningún archivo que no esté registrado corra en el sistema.

5.8.6. Proteger áreas sensibles

Muchos virus tienen la capacidad de "infectar" archivos ejecutables. Con esto se quiere decir que el virus localizará los puntos de entrada de cualquier archivo que sea ejecutable (los archivos de datos no se ejecutan por lo tanto son inutilizables para los virus) y los desviará a su propio código de ejecución. Así, el flujo de

ejecución correrá primero el código del virus y luego el del programa y, como todos los virus poseen un tamaño muy reducido para no llamar la atención, el usuario seguramente no notará la diferencia. Este vistazo general de cómo logra ejecutarse un virus le permitirá situarse en memoria y empezar a ejecutar sus instrucciones dañinas. A esta forma de comportamiento de los virus se lo conoce como técnica subrepticia, en la cual prima el arte de permanecer indetectado.

Una vez que el virus se encuentra en memoria puede replicarse a sí mismo en cualquier otro archivo ejecutable. El archivo ejecutable por excelencia que atacan los virus es el COMMAND.COM, uno de los archivos fundamentales para el arranque en el sistema operativo MS-DOS. Este archivo es el intérprete de comandos del sistema, por lo tanto, se cargará cada vez que se necesite la shell. La primera vez será en el inicio del sistema y, durante el funcionamiento, se llamará al COMMAND.COM cada vez que se salga de un programa y vuelva a necesitarse la intervención de la shell. Con un usuario desatento, el virus logrará replicarse varias veces antes de que empiecen a notarse síntomas extraños en la PC.

El otro "ente" ejecutable capaz de ser infectado es el sector de arranque de los discos magnéticos. Aunque este sector no es un archivo en sí, contiene rutinas que el sistema operativo ejecuta cada vez que arranca el sistema desde esa unidad, resultando este un excelente medio para que el virus se propague de una computadora a la otra. Como se menciono antes una de las claves de un virus es lograr permanecer oculto dejando que la entidad ejecutable que fue solicitada por el usuario corra libremente después de que él mismo se halla ejecutado. Cuando un virus intenta replicarse a un disquete, primero deberá copiar el sector de arranque a otra porción del disco y recién entonces copiar su código en el lugar donde debería estar el sector de arranque.

Durante el arranque de la computadora con el disquete inserto en la disquetera, el sistema operativo MS-DOS intentará ejecutar el código contenido en el sector de booteo del disquete. El problema es que en esa posición se encontrará el código del virus, que se ejecuta primero y luego apuntará el puntero de ejecución a la nueva

posición en donde se encuentran los archivos para el arranque. El virus no levanta sospechas de su existencia más allá de que existan o no archivos de arranque en el sector de booteo.

El virus se encuentra ahora en memoria y no tendrá problemas en replicarse a la unidad de disco rígido cuando se intente bootear desde esta. Hasta que su módulo de ataque se ejecute según fue programado, el virus intentará permanecer indetectado y continuará replicándose en archivos y sectores de booteo de otros disquetes que se vayan utilizando, aumentando potencialmente la dispersión del virus cuando los disquetes sean llevados a otras máquinas.

5.8.7. Aplicar cuarentena

Es muy posible que un programa antivirus muchas veces quede desubicado frente al ataque de virus nuevos. Para esto incluye esta opción que no consiste en ningún método de avanzada sino simplemente en aislar el archivo infectado. Antes de realizar este procedimiento el antivirus reconoce el accionar de un posible virus y presenta un cuadro de diálogo informando acera de la situación actual con el virus. Además de las opciones clásicas de eliminar el virus, aparece ahora la opción de ponerlo en cuarentena. Este procedimiento encripta el archivo y lo almacena en un directorio interno donde se encuentra el antivirus.

De esta manera se está impidiendo que ese archivo pueda volver a ser utilizado y que continúe la dispersión del virus. Como acciones adicionales el antivirus nos permitirá restaurar este archivo a su posición original como si nada hubiese pasado o nos permitirá enviarlo a un centro de investigación donde especialistas en el tema podrán analizarlo y determinar si se trata de un virus nuevo, en cuyo caso su código distintivo será incluido en las definiciones de virus.

5.8.8. Definiciones antivirus

Los archivos de definiciones antivirus son fundamentales para que el método de identificación sea efectivo. Los virus que alcanzaron una considerable dispersión pueden llegar a ser analizados por los ingenieros especialistas en virus de algunas de las compañías antivirus, que mantendrán actualizadas las definiciones permitiendo así que las medidas de protección avancen casi al mismo paso en que lo hacen los virus.

Un antivirus que no este actualizado puede resultar poco útil en sistemas que corren el riesgo de recibir ataques de virus nuevos (como organismos gubernamentales o empresas de tecnología de punta), y están reduciendo en un porcentaje bastante alto la posibilidad de protección. La actualización también puede venir por dos lados: actualizar el programa completo o actualizar las definiciones antivirus. Si contamos con un antivirus que posea técnicas de detección avanzadas, posibilidad de análisis heurístico, protección residente en memoria de cualquiera de las partes sensibles de una unidad de almacenamiento, verificador de integridad, etc., estaremos bien protegidos para empezar. Una actualización del programa sería realmente justificable en caso de que incorpore algún nuevo método que realmente influye en la erradicación contra los virus. Sería importante también analizar el impacto económico que conllevará para nuestra empresa, ya que sería totalmente inútil tener el mejor antivirus y preocuparse por actualizar sus definiciones día por medio si nuestra red ni siquiera tiene acceso a Internet, tampoco acceso remoto de usuarios y el único intercambio de información es entre empleados que trabajan con un paquete de aplicaciones de oficina sin ningún contenido de macros o programación que de lugar a posibles infecciones.

5.9. CARACTERÍSTICAS QUE DEBEN CUMPLIR LOS ANTIVIRUS.

- Deben actualizar los patrones o firmas, por lo menos una vez por semana.
- La empresa que los promueve debe contar con un equipo de soporte técnico con acceso a un laboratorio especializado en códigos maliciosos y un tiempo de respuesta no mayor a 48 horas, el cual me pueda orientar, en mi idioma, en caso de que yo contraiga una infección.

- Deben contar con distintos métodos de verificación y análisis de posibles códigos maliciosos, incluyendo el heurístico, el cual no se basa en firmas virales sino en el comportamiento de un archivo, y así poder detener amenazas incluso de posibles virus nuevos.
- Se deben poder adaptar a las necesidades de diferentes usuarios.
- Deben poder realizar la instalación remota tanto en una red LAN como en una WAN.
- Deben constar de alguna consola central en donde se puedan recibir reportes de virus, mandar actualizaciones y personalizar a distintos usuarios.
- Deben ser verdaderamente efectivos para efectos de detección y eliminación correcta y exacta de los distintos virus que puedan amenazar a los sistemas.
- Deben de permitir la creación de discos de emergencia o de rescate de una manera clara y satisfactoria.
- No deben de afectar el rendimiento o desempeño normal de los equipos, y de ser preferible lo que se desea es que su residente en memoria sea de lo más pequeño.
- El número de falsos positivos que se den tanto en el rastreo normal como en el heurístico debe de ser el mínimo posible.
- Su mecanismo de auto-protección debe de poder alertar sobre una posible infección a través de las distintas vías de entrada, ya sea Internet, correo electrónico, red o discos flexibles, etc.
- Deben de tener posibilidad de chequear el arranque, así como los posibles cambios en el registro de las aplicaciones.

5.10. SOFTWARE ANTIVIRUS.

A continuación se presenta una lista te software antivirus más común disponible:

a. McAfee:

El sistema de seguridad McAfee ofrece diferentes herramientas como por ejemplo el personal firewall plus, virus scan, privacy service y secutiry center. Cada una de ellas es para diferentes necesidades de negocio o personales.

b. Sophos:

Con este software el equipo puede tener escaneados programados o en tiempo real, eliminando las posibilidades de que los virus se extiendan o dañen los datos almacenados. Usuarios remotos y de portátiles ya no tienen por qué ser considerarse un punto débil y con Remote Update se actualiza automáticamente sin necesidad de preocuparse por ello.

c. Panda Software:

Ofrece herramientas para plataformas con windows y linux. Con herramientas que evitan la propagación de códigos maliciosos que utilizan la vulnerabilidad, parándolos directamente en la puerta de entrada del correo electrónico a la empresa y reduciendo, de esta manera, las alertas que los usuarios reciben o la saturación de los buzones de los servidores. Tiene una versión especial para universitarios un área en la que podrán utilizarse las nuevas y exclusivas herramientas gratuitas desarrolladas por Panda Software para la lucha contra los virus informáticos.

d. Per Antivirus:

Detecta y elimina virus en Visual Basic Scripts, Java Scripts, HTML, etc. bajo formatos .VBS, .EXE, .COM, .BAT, .SHS, PIF, SCR, etc. de doble extensión, archivos ocultos, también lo hace en archivos comprimidos en formato ZIP, el más empleado en la transmisión de información vía Internet, correo electrónico o entre diferentes equipos. Detecta y elimina virus activos en memoria, destruyendo cualquier tipo de proceso viral oculto en áreas privilegiadas del sistema operativo, permitiendo un mejor rendimiento y eficacia en la velocidad de desinfección. Integración a MS-Exchange (Server y Cliente), MS-Outlook, Outlook Express, Pegasus Mail, y Lotus Notes (Domino Server), que intercepta los mensajes de correo y revisa antes de que el usuario los abra y lea, eliminando los virus en los archivos anexados, si es que los hubiere.

e. **Proland:**

Sus productos protector plus antivirus son eficientes y fiables, están disponible para Windows y plataformas Exchange Server. Ofrece una base de datos de los virus mas recientes para asegurar la protección de los datos y actualiza el antivirus de las estaciones de trabajo a través de la red.

f. **Symantec:**

Es una de las empresas líderes en cuanto a software antivirus se refiere, escanea el correo electrónico y el tráfico de la Web. Ofrece soluciones de seguridad globales ya sea empresariales y para usuario domestico.

g. **Norman:**

Es un software antivirus que ofrece un amplio rango de herramientas para el control de virus, para integrarla en cada plataforma como OS/2, Windows 95/98/Me, Windows NT/2000/XP/2003, Novell NetWare, MS Exchange, Lotus y Linux. Este antivirus puede identificar y remover todos los tipos de virus incluyendo los sectores de arranque sin que se tenga que reiniciar el equipo con un diskette limpio.

h. **BitDefender:**

La gama BitDefender proporciona protección antivirus para los puntos esenciales de acceso a una red, protegiendo las puertas de enlace, los servidores de Internet, de correo y de archivos y también incluye soluciones antivirus para los usuarios individuales.

i. **Authentium:**

Authentium ha desarrollado soluciones de autentificación y seguridad en los datos de tu empresa, para ambientes de redes y desktop. Tiene un escaneo rápido de virus, una protección dinámica de virus y un completo manejo centralizado para mantener a salvo tu información.

j. **NOD32 de eset:**

NOD32 Anti-Virus System logra un adecuado balance entre el desarrollo actual de los sistemas antivirus y la protección efectiva contra los peligros potenciales que amenazan tu computadora, ejecutándose sobre distintos sistemas operativos como Microsoft Windows 95 / 98 / Me / NT / 2000 / XP, así como en una importante variedad de servidores de correo basados en ambientes UNIX. Virus, gusanos y otros códigos maliciosos son mantenidos a distancia de los valiosos datos contenidos en tu equipo, mediante avanzados métodos de detección, para proporcionar una protección superior incluso sobre aquellos que todavía no han sido desarrollados y/o catalogados.

k. TrendMicro

Sus soluciones protegen el flujo de datos en su PC, servidores de correo electrónico y acceso a Internet. Chequeo en línea.

l. Secuware

Su producto estrella es el "Security Brid Architecture". Protege la información, las comunicaciones, el sistema operativo y todas sus aplicaciones.

m. Kaspersky antivirus

Mundialmente reconocido como uno de los mejores programas en su sector, Kaspersky Anti-Virus, anteriormente conocido como AVP - Antiviral Toolkit Pro, es uno de los programas Antivirus más seguros y fiables del mercado.

5.11. POLÍTICA DE PROTECCIÓN CONTRA VIRUS

Es responsabilidad de cada persona que utiliza la red corporativa de computadoras tomar medidas razonables para proteger la red de infecciones de virus.

5.11.1. Como los virus pueden infectar la red corporativa.

Actualmente existen tres tipos de virus de computadoras: **virus verdaderos, caballos de Troya y los gusanos**. *Los virus verdaderos* actualmente se esconden

ellos mismos, a menudo como macros, dentro de otros archivos, como lo son hojas de cálculos o documentos de Word.

Nota: los virus actualmente pueden esconderse en una variedad de medios diferentes: *aplicaciones, sectores de arranque, sectores de particiones y así sucesivamente.*

Cuando un archivo infectado en abierto desde una computadora que esta conectada a la red corporativa, el virus puede propagarse a través de la red y causar daños. *Un caballo de troya* es un archivo de programa actual que, una vez ejecutado, no se propaga pero puede dañar la computadora donde fue ejecutado. *Un gusano* es también un archivo de programa que, cuando es ejecutado, puede tanto propagarse a través de la red, así como dañar la computadora en donde fue ejecutado.

Los virus de computadoras pueden entrar a la red corporativa de diferentes formas:

- **e-mail:** la mayoría de los virus son enviados como archivos adjuntos en los emails. Estos anexos pueden ser documentos de texto o hojas electrónicas, o pueden ser meramente virus disfrazados como fotos, bromas, etc. Estos anexos pueden haber sido enviados intencionalmente por alguien que quiere infectar la red de corporativa o por alguien que no sabia que el anexo del email contenía un virus. Sin embargo, una vez que el virus es abierto, estos automáticamente se reenvían por correo y el remitente quizás no supo que su computadora estaba infectada con el virus.
- **Discos, CD, Zip drives o otro tipo de almacenamiento:** los virus también se pueden propagar vía varios tipos de almacenamiento. Como con los anexos de un email, los virus se pueden esconder dentro de documentos legítimos o hojas electrónicas o simplemente disfrazarse como otro tipo de archivo.
- **Software bajado desde el Internet:** bajar software vía el Internet puede ser también una fuente de infección. Como en los otros tipos de transmisiones, los virus se pueden esconder dentro de documentos legítimos, hojas electrónicas u otro tipo de archivo.

- **Anexos de mensajes instantáneos**: aunque son menos comunes que los anexos a email. Los virus se aprovechan del software de mensajería instantánea. Estos anexos trabajan de la misma manera que los virus de email, pero estos son transmitidos vía software de mensajes instantáneos.

5.11.2. Como el departamento de informática de la organización prevee o minimiza las infecciones de virus.

El departamento de informática de la organización lucha con los virus en diferentes formas:

a. **Analizando el tráfico de Internet:** todo el tráfico de Internet entrante y saliente desde la red corporativa debe pasar a través de los servidores de la organización y otros dispositivos de red. Solamente los tipos específicos de tráfico de red son permitidos más allá de los firewalls exteriores de la organización.

   Por ejemplo, un mensaje de email que se origina afuera de la red debe pasar a través del servidor antivirus y el firewall instalado en la organización primero antes de que este sea permitido a entrar en el servidor de correo electrónico interno. Este dispositivo enruta los emails sospechosos y anexos hacia un dispositivo de almacenamiento aislado, de esta manera se derrota el propósito del virus, el cual es entrar en la red corporativa.

b. **Utilizando servidores y estaciones de trabajo con software antivirus:** todos los servidores vulnerables corren el software antivirus que la corporación posee. Este software analiza los almacenamientos de datos con información compartida con el propósito de encontrar código sospechoso.

   El software antivirus también es instalado en todas las estaciones de trabajo de la organización. Este software analiza todos los datos escritos o leídos en los discos duros de las estaciones de trabajo. Si este software encuentra algo sospechoso,

este aísla el archivo dudoso en la computadora y automáticamente notifica al departamento encargado de manejar estos problemas. Por ejemplo, helpdesk.

c. **Actualizando la definición de virus constantemente:** cada mañana, el firewall y el servidor antivirus corren programas que buscan actualizar la definición de virus del software antivirus a través del servidor destinado para las actualizaciones por parte del fabricante del software antivirus. Estos archivos de definición permite al software detectar nuevos virus. Si un archivo de definición de virus esta disponible, el software antivirus es actualizado automáticamente, y el administrador del sistema es informado.

   Cuando los usuarios encienden sus estaciones de trabajo al principio del día laboral, los programas de protección contra virus instalados en las estaciones de trabajo chequean con el servidor antivirus si una nueva actualización esta disponible, si esta disponible, la estación de trabajo baja la actualización, esta se actualiza automáticamente y el administrador del sistema es informado.

5.11.3. Como responder o reportar la presencia de un virus.

Aunque todo el tráfico de Internet es analizado en busca de virus y todos los archivos de la corporación son analizados también, existe aun la posibilidad de que un nuevo o bien escondido virus pueda encontrar el camino para llegar a la estación de trabajo del usuario y si no es manejado propiamente, este podría infectar la red corporativa.

El personal del departamento de informática intentara notificar a todos los usuarios de la amenazas virus existentes vía email o por mensajes telefónicos. Debido a que esta notificación ira a todos los miembros de la corporación, los empleados no deben reenviar los mensajes de advertencias de virus. En ocasiones, personas mas conocedoras distribuirán mensajes de advertencias de virus los cuales son virus falsos, sin embargo, reenviar tales mensajes innecesariamente incrementa el tráfico de la red.

Como se planteo anteriormente, es responsabilidad de todos los usuarios de la red corporativa el tomar pasos razonables para prevenir problemas con los virus. A continuación se mencionan algunas guías que los usuarios pueden seguir para lograr este objetivo:

- No abrir emails inesperados con archivos anexos, aun cuando un colega lo ha enviado.
- Nunca abrir un email o mensaje instantáneo con archivos anexos desde orígenes sospechosos o desconocidos.
- Nunca bajar software gratis o compartido desde el Internet sin el debido consentimiento y autorización del departamento de informática de la corporación.
- Si se recibe un archivo que contiene macros y no se esta seguro este, los macros deben ser deshabilitados.

5.11.4. Notificar al departamento encargado de manejar problemas con Virus (helpdesk) cuando se han detectado archivos sospechosos.

Si se recibe un archivo sospechoso o un correo electrónico con un archivo adjunto de dudosa procedencia, este no debe abrirse. Se tiene que notificar o llamar al departamento encargado (helpdesk) e informar al analista de soporte(o persona encargada) de que se ha recibido un archivo sospechoso. El analista de soporte explicara como manipular este archivo.

Si el archivo que esta infectado es una hoja electrónica o un documento que es de suma importancia para la organización, el departamento de informática intentara analizar y limpiar el archivo. El departamento de informática, sin embargo, no garantiza si el archivo infectado sea limpiado completamente, de no ser así, no permitirá que el archivo infectado sea usado en las computadoras de la red.

5.12. ESTRATEGIAS DE SEGURIDAD ANTIVIRUS:

A continuación se presentan de forma general algunas estrategias.

5.12.1. Estrategias generales de seguridad antivirus

- Un solo proveedor de software antivirus reduce la sobrecarga de configuración y mantenimiento en el departamento de informática. Un solo paquete es preferible pero no siempre es posible, especialmente si mas de un sistema operativo esta involucrado.
- La administración centralizada ayuda a minimizar la demanda del equipo de soporte del departamento de informática al eliminar visitas por cambios de configuración y actualizaciones. Esta también provee un solo punto para la diseminación controlada para la actualización de definiciones y motores, así también, permite que la misma configuración sea aplicada a todas las computadoras similares. Una opción basada en explorador permite el acceso desde cualquier computadora, así el administrador puede ser mas flexible o ágil con los problemas del usuario final.
- La habilidad de realizar la instalación inicial, actualizaciones y configuraciones por parte de los clientes reduce el tiempo productivo dentro de la empresa debido al tiempo requerido para realizar estas tareas. La entrega automática del software y las actualizaciones sin la iteración de los usuarios es preferida; el usuario no debería tener la oportunidad de comprometer o detener la instalación. Si una computadora es apagada o desconectada durante el proceso de instalación/actualización, el software debería de ser capaz de continuar o reiniciar la siguiente vez que el usuario entre al sistema.
- Ser capaz de detectar nodos desprotegidos reduce la posibilidad de olvidar la instalación del paquete antivirus en una computadora en particular. Esto es particularmente importante en un ambiente en el cual computadoras que no pertenecen a la corporación se les es permitido conectarse a la red. Idealmente, el software administrativo debería ser capaz de alertar inmediatamente al administrador de red cuando un nodo desprotegido es

descubierto, para prevenir el ataque de un nodo desprotegido e inmediatamente forzar la instalación del software en el nodo. Estas funciones deberían ser todas configurables para lograr las necesidades de el ambiente específico.

- La efectividad de cualquier software antivirus es grandemente disminuida si el usuario final puede apagar la protección por propia voluntad. Si el usuario tiene acceso para cambiar la configuración, especialmente para excluir que archivos ciertos archivos sean escaneados, la protección esta seriamente comprometida.
- Algunas veces, los usuarios pueden deshabilitar temporalmente la protección antivirus para usar sus computadoras. Cuando un usuario esta trabajando remotamente y esta desconectado de la red corporativa, debería ser posible introducir un passoword provisto por el departamento de informática para encender o apagar la protección contra virus.
- Independientemente de cuando es usuario es actualizado desde el servidor administrativo o desde Internet, ambos motores y actualizaciones de definiciones deberían correr silenciosamente sin la intervención del usuario final. Para proveer protección confiable, la solución antivirus debería operar independientemente de las acciones del usuario final y con la mínima confianza en el personal del departamento de informática. Si los usuarios ven las actualizaciones corriendo, esto inevitablemente resultara en mas llamadas hacia el departamento de informática por parte de los usuarios preguntándose que esta sucediendo, es por esto que las actualizaciones silenciosas son preferidas.
- Tiempo de entrega garantizado para desinfectar un nuevo virus detectado es crítico porque un paquete antivirus puede proteger a un cliente solamente contra virus conocidos o aquellos que fallan en evadir el análisis heurística.
- El personal de informática necesita la habilidad de controlar cuando las actualizaciones de definiciones son entregadas a los clientes y como anular el horario para continuar con la siguiente actualización. Para máxima protección, el proveedor de soluciones antivirus idealmente debería estar permitido para entregar actualizaciones de definiciones nuevas a todos los clientes tan pronto

como estén disponibles. Sin embargo, dependiendo de las restricciones que operan en la red corporativa, esto no siempre es práctico o deseable.

Por lo tanto el administrador debería ser capaz de controlar cuando los clientes reciben actualizaciones de definición directamente desde el proveedor o desde un servidor administrativo y en que horario.

- No es suficiente simplemente con controlar el nivel de protección de las computadoras clientes dentro de una red. Es también deseable ser capaz de negar el acceso a clientes remotos que no tienen las definiciones de virus mas recientes. Las computadoras portátiles representan una amenaza de virus considerable, no siempre es posible controlar el ambiente en el cual les es permitido conectarse en las afueras de su red propia. Es irreal confiar en la diligencia del usuario final para asegurar que la computadora esta libre de virus antes de hacer la conexión remota a la red interna. Por lo tanto cualquier solución antivirus debe ser capaz de comunicarse con la solución de acceso remoto para denegar el acceso hacia clientes protegidos inadecuadamente.
- Es un complemento esencial a los requerimientos previos. Si a las computadoras remotas se les puede negar el acceso por no tener la definición de virus mas reciente, estos deben ser capaces de actualizarse directamente desde el proveedor de la solución vía Internet. Esta solución antivirus no puede ser permitido que afecte la habilidad del usuario para desarrollar su función de trabajo.
- Los horarios de escaneo por defecto no son prácticos para todos los ambientes. El administrador necesita la habilidad para programar escaneos basados en grupos específicos. Los escaneos afectan negativamente el desempeño de las computadora, para algunos usuarios, es razonable realizar esta actividad durante las horas de trabajo, para otros usuarios no lo es. Los escaneos en la noche son deseables si la política actual permite que las computadores permanezcan encendidas, pero claramente estas no son prácticas para dispositivos portátiles.
- Desde un punto de vista de protección, siempre es preferible realizar un escaneo en el arranque de la computadora. La solución antivirus debería tener esta posibilidad como una opción configurable basados en grupos específicos.

- No todos los tipos de archivos pueden ser infectados y al excluir estos tipos de archivos de todos los escaneos puede reducir negativamente el desempeño del usuario final. Por la misma razón, debe también probar necesariamente excluir los archivos sobre un cierto tamaño o archivos que están almacenados en ciertas localidades.
- Descargas desde la web y distribuciones vía e-mail se han convertido en el método preferido para la diseminación de virus, por lo tanto protección completa para estos (y todos los demás) puntos accesos es esencial. El paquete debería ser capaz de escasear tanto los e-mails entrantes como salientes y filtrar todo el tráfico web.
- El análisis heurístico provee protección esencial contra virus en los cuales una definición no esta disponible todavía. Si este análisis, es solamente tan efectivo como sus ultima actualización de definición.
- En algunos ambientes o circunstancias, podría ser deseable para miembros del departamento de informática ser alertados en el instante en que el virus es detectado.
- Inevitablemente, una infección ocurrirá. Pero teniendo las herramientas para manejar el comienzo de la infección de una manera completa y lógica se puede grandemente reducir el impacto de semejante ocurrencia.
- Comprensivamente, los reportes personalizados con la actividad de los virus a través de la organización son una herramienta invaluable para justificar el costo de proveer protección antivirus a los administradores superiores. Los reportes deberían ser fáciles de entender, mostrar al mínimo, el numero de virus detectados dentro de un periodo determinado, donde un virus fue detectado y una breve descripción de los efectos esperados de los virus si estos no hubiesen sido evitados. El personal del departamento de informática también necesita reportes para mostrar cuales archivos han sido puestos en cuarentena o eliminados para permitirles ayudar a los usuarios finales en el reemplazo de los archivos perdidos.

5.12.2. Responsabilidades del administrador de red:

- Instalar y mantener el software antivirus apropiado en todas las computadoras de la red corporativa.
- Responder a todos los ataques de virus, destruir cualquier virus detectado y documentar cada incidente.
- Configurar el software antivirus con el objetivo de que este sea capaz de auto-actualizarse siguiendo una base de tiempo determinada.
- Configurar el servidor antivirus con el objetivo escanear las computadoras en segundo plano sin afectar el rendimiento o desempeño del usuario.
- Configurar el servidor antivirus con el objeto de realizar un escaneo completo de la computadora siguiendo una base de tiempo determinada, preferiblemente durante las horas de no trabajo

5.12.3. Responsabilidades del empleado:

- Los empleados no introducirán de manera intencional un virus de computadora en cualquier computadora de la compañía.
- Los empleados no utilizaran ningún diskette proveniente de un origen desconocido.
- Los diskettes que han sido introducidos a la compañía serán analizados en busca de virus antes de ser utilizados.
- Cualquier empleado que sospeche que su estación de trabajo ha sido infectada por un virus apagara inmediatamente su estación de trabajo y llamara a su administrador de red.
- Nunca abrir un archivo que sea haya recibido por correo electrónico y el usuario no este seguro de la clase de archivo se trata y/o el propósito de este, aunque provenga de una persona conocida.
- Nunca abrir archivos que han sido enviados por un desconocido cuando se utilice cualquier software para mensajera rápida. Ej.: Messenger.

Programas permitidos para descargar desde Internet dentro de la red corporativa:

- AOL Instant Messenger
- ICQ
- Winzip
- Ad-aware
- Spybot
- RealOne Player
- Adobe Acrobat Reader, Adobe Reader
- Slimbrowser
- Microsoft windows media player, winamp
- quicktime
- aplicaciones para ebooks
- aplicaciones antispams

Programas denegados para descargar desde Internet dentro de la red corporativa:

- kazaa media desktop
- imesh
- morpheus (todas las versiones)
- winmx
- limewire
- grokster
- bearshare
- zonealarm
- cualquier salvapantallas de terceras compañías
- juegos para computadora

5.13. SPYWARE.

El spyware es un problema muy cumun en la seguridad de las organizaciones. A continuación se explica de una manera breve que es el spywere y las formas de como se puede prevenir.

5.13.1. ¿Que es un spyware?

Tanto maligno como benigno, spyware es un software secretamente colocado en una computadora que registra y reporta la actividad del usuario.

5.13.2. ¿Como infectase?

- **Cookies:** muchos sitios Web legítimos utilizan las cookies de manera apropiada. Sitios web maliciosos pueden sin embargo utilizar las cookies para recopilar y reportar la actividad del usuario para propósitos dudosos.
- **Instalación a través de sitios web:** sitios Web maliciosos a menudo disfrazan el spyware como una herramienta de ayuda y conducen al usuario a instalar el spyware cuando se visita el sitio Web.
- **Archivos adjuntos en los emails o enlaces:** como con los virus, spyware puede propagarse como un archivo adjunto en un email o enlace.
- **Accesorios de aplicaciones:** frecuentemente incluido en un software popular, como los son las aplicaciones peer-to-peer, juegos libres, herramientas para remover spyware telefónico y cosas parecidas. Este puede o no ser revelado durante el proceso de instalación de la aplicación.

5.13.3. Señales de infección

- Reducción inexplicable en el desempeño de la computadora.

- Aparición de nuevas barras de herramientas que no pueden ser eliminadas permanentemente.
- Trafico de red/MODEM inexplicable y excesivo
- Incremento dramático de ventanas relacionadas con publicidad
- Cambio en el motor de búsqueda o pagina inicial por defecto del explorador de Internet.

5.13.4. Remoción de Spyware

- Identificar y finalizar procesos sospechosos con el administrador de tareas de Windows.
- Identificar y deshabilitar servicios sospechosos con el administrador de consola.
- Identificar y deshabilitar servicios y programas de arranque en Windows con la utilidad de configuración del sistema.
- Buscar y borrar entradas de registro asociadas con servicios sospechosos o programas de arranque.
- Identificar y borrar archivos sospechosos
- Instalar y usar múltiples utilidades para detectar y remover spyware.

5.13.5. Prevención contra spyware

- Aplicar regularmente actualizaciones y parches de software
- Cuando sea posible, configurar las cuentas de usuario sin descargar o instalar permisos
- Prohibir la instalación y uso de software no aprobado particularmente relacionado con la transferencia de archivos peer-to-peer
- Usar utilidades comerciales seguras
- Regularmente escanear las computadoras con programas antivirus y antispyware

- Usar el firewall para restringir el tráfico saliente en todos los puertos excepto aquellos utilizados para http, pop3, smtp.
- Limitar el acceso web solamente a aquellos sitios seguros mediante el uso de servidores proxy o restringir la lista de sitios permitidos.
- Ajustar las configuraciones de permiso para las cookies y zonas de seguridad el explorador de Internet.

CAPITULO 6. ROUTERS

Los routers son la primera y última línea de defensa en la cual se apoya la estrategia de seguridad “Defensa en profundidad” porque controlan, dirigen y restringen el tráfico tanto entrante como saliente entre la red corporativa confiable y la red pública no confiable (Internet).

El presente capitulo enseña como la seguridad de redes es fortalecida mediante el estudio de temas como el filtrado de paquetes y lista de control de acceso, brindando información relevante acerca del porque de su utilización, aporte a la seguridad y recomendaciones acerca de que protocolos o servicios deberían ser restringidos a fin de proporcionar una línea de defensa mas en la aplicación de la estrategia de seguridad “Defensa en profundidad”.

Puntos clave:

- Mencionar características principales de los routers
- Describir los motivos para crear seguridad con los routers
- Detallar como los routers forman parte de la estrategia “defensa en profundidad”
- Detallar las funciones del router tanto a nivel físico como lógico

Un router es un conmutador de paquetes que opera en la capa de red del modelo OSI.

Sus principales características son:

- Permiten interconectar tanto redes de área local como redes de área extensa.
- Proporcionan un control del tráfico y funciones de filtrado a nivel de red, es decir, trabajan con direcciones de nivel de red, como por ejemplo, con direcciones IP.
- Son capaces de encaminar dinámicamente, es decir, son capaces de seleccionar el camino que debe seguir un paquete en un momento necesario, teniendo en cuenta factores como líneas más rápidas, líneas más baratas, líneas menos saturadas, etc.

6.1 MOTIVOS PARA CREAR SEGURIDAD CON ROUTERS.

Los routers proveen servicios que son esenciales para la operación correcta y segura de las redes a las que ellos sirven. El compromiso de un router puede conducir a varios problemas de seguridad en las redes servidas por esos routers, o aun en otras redes con las cuales este router se comunica.

- El compromiso de las tablas de enrutamiento de un router puede resultar en una reducción en el desempeño, negación de los servicios de comunicación de la red, y la exposición de datos sensitivos.
- El compromiso del control de acceso de un router puede dar como resultado exposición de detalles de configuración de la red o negación del servicio y puede facilitar ataques en contra de otros componentes de la red.
- Un router con una configuración de filtrado pobre puede reducir la seguridad global de un enclave entero, es decir puede exponer componentes internos de la red para examinar y atacar, así también puede hacer mas fácil para los atacantes el evitar la detección.

- Por otra parte, el uso correcto de las funciones de seguridad criptográficas de un router puede ayudar a proteger datos sensitivos, puede asegurar la integridad de los datos y puede facilitar la cooperación segura entre enclaves independientes.

En general, los routers bien configurados pueden grandemente mejorar la postura de seguridad global de una red. La política de seguridad implementada en un router es difícil de evadir para usuarios finales negligentes o maliciosos, por lo tanto se evita una fuente potencial muy seria de problemas de seguridad.

6.2. LOS ROUTERS COMO PARTE DE DEFENSA EN PROFUNDIDAD.

6.2.1 Roles de los routers en las operaciones y seguridad de la red

En una red de computadoras muy pequeña, es factible utilizar mecanismos simples secuénciales o de transmisión para mover datos desde punto a otro. Una red de área local Ethernet (LAN) es esencialmente una red de transmisión. En redes mayores y más complejas los datos deben ser dirigidos específicamente hacia el destino pretendido. Los routers dirigen los mensajes de datos de la red o paquetes, basados en tablas de rutas y direcciones internas, o destinos conocidos que sirven ciertas direcciones. Dirigir datos entre porciones de una red es el propósito primario de un router. Las redes de computadoras más grandes usan el conjunto del protocolo TCP/IP.

La figura 6.1 ilustra la función primaria de un router en una red IP pequeña.

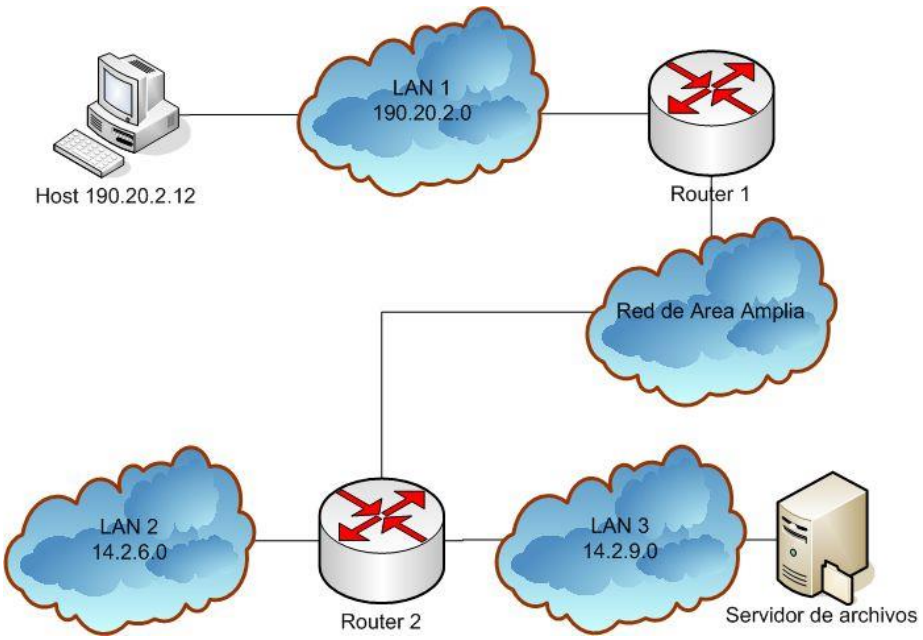


Figura 6.1. Una red simple con dos routers

Si el host (arriba a la izquierda) necesita enviar un mensaje al servidor de archivo (fondo a la derecha), crea un paquete con dirección 14.2.9.10, y envía el paquete sobre la LAN 1 a su gateway, Router 1. Consultando su tabla interna de ruta, el Router 1 reenvía el paquete hacia el Router 2. Consultando su propia tabla de ruta, el Router 2 envía el paquete sobre la LAN 3 al Servidor de Archivo. En la práctica, la operación de cualquier red grande depende de las tablas de ruta en todo sus routers constituyentes. Sin enrutamiento robusto, la mayoría de redes modernas no pueden funcionar. Por consiguiente, la seguridad de routers y sus especificaciones de configuración es vital para la operación de la red.

a. Routers Interiores

Un router interior reenvía tráfico entre dos o más redes locales dentro de una organización o empresa. Las redes conectadas por un router interior a menudo comparten la misma política de seguridad y el nivel de confianza entre ellos es usualmente alto. Si una empresa tiene muchos routers interiores, estos usualmente emplearan un protocolo IGP (Interior Gateway Protocol) para manejar las rutas. Los routers interiores pueden imponer algunas restricciones en el tráfico que estos reenvían entre las redes.

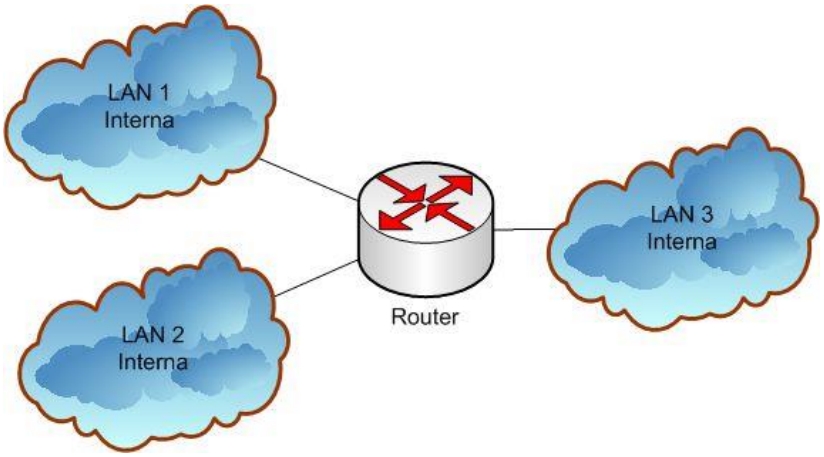


Figura 6.2. Un router interior que conecta las redes internas de la organización

b. Routers Backbone

Un router backbone o exterior es uno que reenvía el tráfico entre diferentes empresas (algunas veces llamadas “sistemas autónomos”). El tráfico entre las diferentes redes que hacen el Internet está dirigido por los routers backbone.

El nivel de confianza entre las redes conectadas por un router backbone usualmente es bastante bajo. Típicamente, los routers backbone están diseñados y configurados para reenviar datos tan rápido como sea posible, sin imponer ninguna restricción. Los objetivos de seguridad primarios para los routers backbone son el asegurar que la administración y operación de los routers este conducida solamente por partes autorizadas y proteger la integridad de la información de enrutamiento que este usa para reenviar el tráfico. Los routers backbone típicamente emplea el Protocolo de Gateway Exterior.

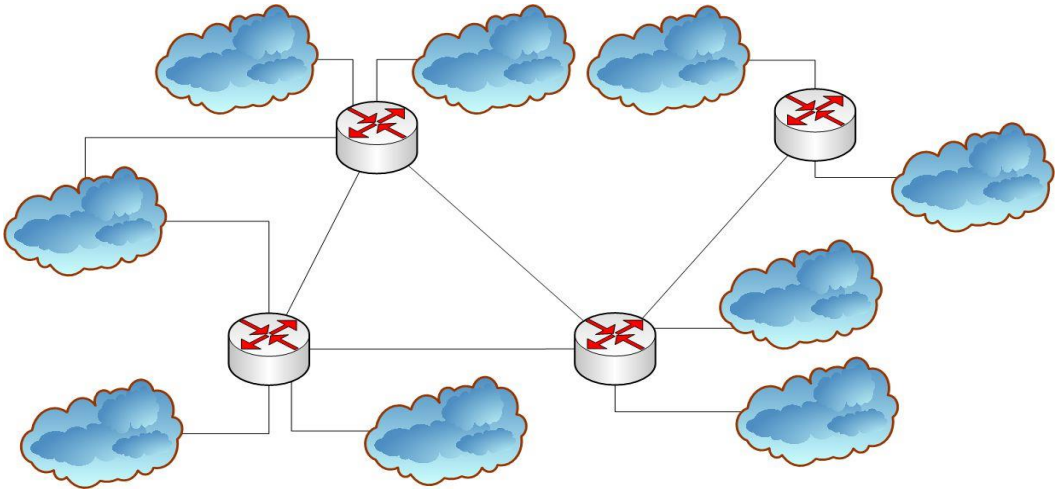


Figura 6.3. Routers backbone que pueden conectar muchas redes.

c. Routers *de* perímetro

Un router de perímetro reenvía el tráfico entre una empresa y las redes exteriores. El punto clave de un router de perímetro es que éste forma parte de los límites entre la red interna confiable de una empresa y la red externa no confiable (ej. El Internet). El router de perímetro puede ayudar a asegurar el perímetro de la red de una empresa al imponer restricciones en el tráfico que controla. Un router de perímetro puede emplear protocolos de enrutamiento o puede depender enteramente de rutas estáticas.

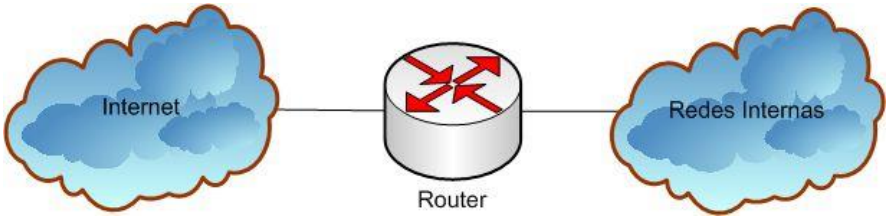


Figura 6.4. El router de perímetro conecta las redes internas a una red externa

Típicamente, un router de perímetro no es el único componente en el límite; muchas empresas también emplean un firewall para reforzar la política de seguridad.

En la siguiente figura, el router de perímetro actúa como la primera línea de defensa y es conocido como router de filtrado. Este contiene una ruta estática por la cual pasan todos los intentos de conexión hacia la red protegida a través del firewall. El firewall provee control de acceso adicional sobre las conexiones y el tráfico de la red. El firewall puede también realizar autenticación de usuarios. Usar un firewall y un router juntos puede ofrecer una mejor seguridad que cualquiera de los dos por separado.

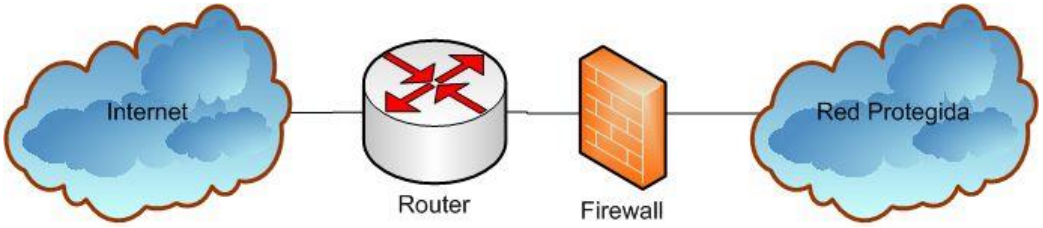


Figura 6.5. Uso del Firewall

Otra aproximación es posicionar un router en la conexión entre las redes externas y entonces colocar otro router entre el firewall y la red interna confiable. Esta configuración ofrece dos puntos en los cuales las políticas pueden ser implementadas. Esto también ofrece una área intermedia, a menudo llamada *la zona desmilitarizada o DMZ* entre los dos routers. La DMZ es a menudo utilizada por servidores que deben ser accesibles desde el Internet u otra red externa.

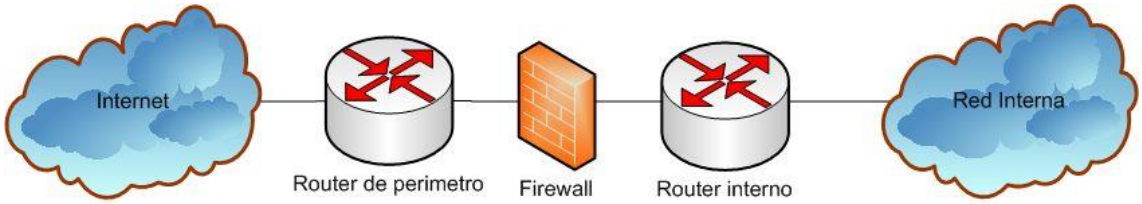


Figura 6.6. Proyección de la red interna con Routers y Firewalls

6.2.2. Filtros de paquetes para TCP/IP.

Un filtro de paquete para servicios TCP/IP provee control de la transferencia de datos entre las redes basadas en direcciones y protocolos. Los routers pueden aplicar filtros en formas diferentes, algunos routers tienen filtros que aplican a los servicios de red tanto en dirección entrante como saliente desde la red, mientras que otros filtros tienen que ser aplicados solamente en una dirección. Muchos servicios son bidireccionales, por ejemplo, un usuario en un sistema A hace una conexión telnet hacia un sistema B y el sistema B envía algún tipo de respuesta de regreso al sistema A. Por lo tanto, algunos routers necesitan dos filtros para manejar los servicios bidireccionales. La mayoría de los routers pueden filtrar uno o mas de los siguientes elementos: dirección IP origen, puerto origen, dirección IP destino, puerto destino y tipo de protocolo. Algunos routers pueden aun filtrar cualquier bit o patrón de bits en el encabezado IP. Sin embargo, los routers típicamente no tienen la capacidad para filtrar el contenido de los servicios, ejemplo: el nombre del archivo a través de FTP.

Los filtros de paquetes son especialmente importantes para los routers que actúan como una entrada entre las redes confiables y no confiables. En ese papel, el router

puede implementar la política de seguridad, rechazando protocolos y restringiendo los puertos de acuerdo a las políticas de la red confiable. Los filtros también son importantes por su habilidad para implementar restricciones de direccionamiento. Por ejemplo en la figura mostrada en la sección de routers interiores, el router debería implementar la restricción que paquetes enviados desde la red interna o protegida (derecha o izquierda) debe encarar una dirección origen dentro de un rango particular. Esto es llamado a menudo *filtrado de salida.* Similarmente el router debería implementar una restricción para que los paquetes que llegan desde el Internet debe encarar una dirección origen afuera del rango valido para la red protegida. Esta es una forma de *filtrado de entrada.*

Las dos características principales del filtrado de paquetes TCP/IP son la longitud y el ordenamiento. Un filtro consiste de una o más reglas, en donde cada regla acepta o niega un cierto número de paquetes. El número de reglas en un filtro determina su longitud. Generalmente, cuando la longitud crece en el filtro este se hace más complejo para reparar cuando sucede algún problema.

6.2.3 Aplicando filtros de paquetes: permitir ciertos protocolos o servicios

Hay que considerar muy cuidadosamente que servicios de red serán permitidos a través del router (entrada y salida) y para el router. Es posible mediante el uso de la siguiente guía para la creación de filtros: **aquellos servicios que no están permitidos explícitamente son prohibidos.** Este guía es especialmente importante para routers de perímetro. Se debe realizar una lista de todos los servicios y protocolos que deben cruzar el router y aquellos que el router mismo necesita para su operación. Se debe crear un conjunto de reglas de filtrado que permite el trafico identificado en la lista y prohibir todo el trafico restante.

En casos donde solamente ciertos clientes o redes necesitan acceso a servicios particulares se debe agregar una regla de filtrado que permite ese servicio pero solamente para direcciones de clientes o rangos de direcciones específicos. Por

ejemplo el cliente firewall de la red puede ser la única dirección autorizada para iniciar conexiones Web (TCP puerto 80) a través del router.

6.2.4 Aplicando filtros de paquetes: rechazando protocolos y servicios riesgosos.

Algunas veces no es posible seguir una guía estricta de seguridad como la discutida anteriormente. En este caso, se hace referencia a los servicios prohibidos que no son comúnmente necesitados o son conocidos también por ser vehículos populares que comprometen la seguridad de la red. Las siguientes dos tablas presentan los servicios mas comunes que son restringidos debido a que son utilizados para recolectar información acerca de la red protegida o tienen debilidades que pueden ser explotadas en contra de la red protegida. La primera tabla lista aquellos servicios que deberían ser completamente bloqueados por un router de perímetro típico. A menos que se tenga una necesidad operacional específica para soportarlos, los protocolos listados a continuación no deberían ser permitidos que pasen por el router en ninguna dirección:

6.2.5 Servicios que se deben bloquear completamente en un router de perímetro.

Puerto (Transporte)	Servicio
1 (TCP & UDP)	Tcpmux
7 (TCP & UDP)	Echo
9 (TCP & UDP)	Discard
11 (TCP)	Systat
13 (TCP & UDP)	Daytime
15 (TCP)	Netstat
19 (TCP & UDP)	Chargen
37 (TCP & UDP)	Time
43 (TCP)	Whois
67 (UDP)	Bootp
69 (UDP)	Tftp
95 (TCP & UDP)	Supdup
111 (TCP & UDP)	Sunrpc

135 (TCP & UDP)	loc-srv
137 (TCP & UDP)	netbios-ns
138 (TCP & UDP)	netbios-dgm
139 (TCP & UDP)	netbios-ssn
177 (UDP)	Xdmcp
445 (TCP)	netbios (ds)
512 (TCP)	Rexec
515 (TCP)	Lpr
517 (UDP)	Talk
518 (UDP)	Ntalk
540 (TCP)	Uucp
1434 (UDP)	Microsoft SQL Server
1900, 5000 (TCP & UDP)	Microsoft UPnP SSDP
2049 (UDP)	NFS
6000 - 6063 (TCP)	X Window System
6667 (TCP)	IRC
12345-6 (TCP)	NetBus
31337 (TCP & UDP)	Orificio Trasero

Tabla 6.1 Servicios bloqueados por el router

La siguiente lista muestra algunos servicios en una red interna o en el router mismo que no deberían ser accesados para conexiones desde adentro de la organización:

6.2.6 Algunos servicios a bloquear en el router para clientes externos

Puertos (Transporte)		Servicio
79	(TCP)	Finger
161	(TCP & UDP)	Snmp
162	(TCP & UDP)	snmp trap
513	(TCP)	rlogin
513	(UDP)	Who
514	(TCP)	rsh, rcp, rdist, rdump
514	(UDP)	Syslog
50	(TCP & UDP)	Ne

Tabla 6.2 Servicios bloqueados por el router para clientes externos

6.2.7 Filtrado de direcciones.

Los filtros de los routers también deberían usarse para protegerse contra los ataques hacia la dirección IP, especialmente en routers de perímetro. En muchos casos las reglas de filtrado deberían aplicar filtrado para la admisión y salida de datos, así también incluir el bloqueo para direcciones reservadas. Los principios a aplicar en los routers de perímetro son listados a continuación:

- Rechazar todo tráfico desde las redes internas que tienen una dirección IP origen que no forma parte de las redes internas. (El tráfico legítimo generado por los orígenes en las redes internas siempre llevara una dirección de origen que esta dentro del rango o los rangos asignados para las redes internas; Cualquier otro tráfico intenta reclamar una dirección falsa desde el origen es casi ciertamente erróneo o malicioso por la naturaleza.)
- Rechazar todo tráfico desde las redes externas que tiene una dirección origen que forma parte de las redes internas. (Dado que las direcciones están asignadas correctamente, el tráfico enviado de las redes externas siempre debería cargar una dirección origen de algún rango aparte de los asignados para las redes internas. El tráfico que presenta tales direcciones corrompidas es a menudo parte de un ataque y debería ser descartado por un router de perímetro.
- Rechazar todo tráfico con un origen o dirección destino que pertenecen a cualquier el rango reservado, no enrutable o un rango de direcciones ilegales.

6.2.8 Mitigando el ataque de negación de servicios

La pérdida de servicio o desempeño de la red gravemente degradado puede resultar de una variedad de causas. La negación de servicios (DoS) se refiere a los intentos deliberados para causar tales interferencias. Aunque los ataques DoS pueden ser mirados como molestias tolerables, pueden tener consecuencias serias si ocurren durante un tiempo de crisis. No hay una solución completa para erradicar el problema

de DoS; Mientras los recursos de una red están limitados y abiertamente disponibles serán vulnerables para atacar. Hay medidas que los administradores de red pueden tomar para proteger las redes de ataques DoS y reducir sus efectos. Estas medidas requieren un esfuerzo cooperativo entre aquellos que administran los clientes, los dispositivos de red y proveen acceso. Para ser efectivas, estas medidas deben ser planeadas y ejecutadas antes de que un ataque ocurra.

A nivel empresarial hay tres estrategias primarias para combatir los ataques de DoS y son descritos a continuación:

- Prevenir que el tráfico malicioso no entre en la red común corporativa.
- Configurar y desplegar medidas protectoras locales tanto en los routers exteriores como interiores.
- Coordinar medidas protectoras contra ataques distribuidos de DoS con proveedores de acceso de red y/o administradores de backbones..

6.3 LISTAS DE CONTROL DE ACCESO – ACL

Las listas de acceso en los routers Cisco proveen la capacidad de filtrado y selección de paquetes. Una lista de acceso consiste en una o mas reglas. Para tráfico IP, existen dos tipos de listas de acceso disponibles: la estándar y la extendida.

Las listas de acceso estándar solamente permiten el filtrado de las direcciones IP origen. Las listas de acceso extendidas pueden permitir o denegar paquetes basados en sus protocolos, direcciones IP origen o destino, puertos TCP/UDP origen o destino, mensajes de tipo ICMP o IGMP. Las listas de acceso extendidas también soportan logins selectivos. Tanto la listas de acceso IP estándar o extendida puede ser aplicada a las interfaces del router, líneas vty (para acceso remoto), IPSec, protocolos de enrutamiento y muchas otras funciones del router. Solamente las listas de acceso IP estándar pueden ser aplicadas a SNMP.

Sintaxis:

La estructura básica de la lista de acceso es mostrada a continuación:

access-list *numero-de-lista* {**deny | permit**} *condición.*

El número de lista de acceso le comunica al IOS de Cisco de que lista de acceso la regla debería ser parte. El campo condición, el cual es diferente para cada lista de acceso, especifica que paquetes deben cumplir con la regla. Las condiciones típicamente involucran información de protocolos y direcciones, pero no involucran información a nivel de aplicación.

El siguiente es un ejemplo de la sintaxis para el establecimiento de una regla en una lista de acceso IP estándar:
access-list *numero-de-lista* {**deny | permit**} *origen* [*comodin-origen*] [**log**]

donde
numero-de-lista es el numero de la lista de acceso y puede ser cualquier numero decimal entre 1 hasta 99.

deny deniega el acceso si la condición es cierta.
permit permite el acceso si la condición es cierta.

Origen es la dirección IP de la red o el host de donde el paquete ha sido enviado.
comodin-origen es el comodin de bits que se aplican al origen.

La palabra clave opcional **log** puede ser aplicada para registrar las combinaciones exitosas con la regla. Nota: esta función es soportada solamente por IOS 12.0 o superiores.

El siguiente es un ejemplo de la sintaxis para el establecimiento de una regla en una lista de acceso IP extendida:

access-list *numero-de-lista* {**deny | permit**} *protocolo origen comodin-origen calificadores-destino destino comodin-destino calificadores-destino* [**log | log-input**]

donde:
numero-de-lista es el numero de la lista de acceso y puede ser cualquier numero decimal entre 1 hasta 99.

deny deniega el acceso si la condición es cierta.
permit permite el acceso si la condición es cierta.

Protocolo es el nombre o numero de un protocolo IP relacionado, puede ser una de las siguientes palabras claves: eigrp, gre, icmp, igmp, igrp, ip, ipinip, nos, ospf, tcp o udp. O puede ser un entero entre el rango de 0 hasta 255 representando el numero del protocolo IP. (Algunos protocolos permiten calificadores adicionales: puertos origen o destino que pueden ser especificados para tcp o udp y tipos de mensajes que pueden ser especificados para icmp o igmp).

Origen es la dirección IP para la red o host de donde el paquete ha sido enviado.

comodin-origen es el comodin de bits para ser aplicados en el origen. La palabra clave **any** puede ser usada en lugar en lugar de origen y comodin-origen.

calificadores-origen son detalles opcionales en el paquete origen, incluyendo numero de puertos y otra información especifica del protocolo.
destino es la dirección IP para la red o host hacia donde el paquete ha sido enviado.
comodin-destino es el comodin de bits para ser aplicados en el destino. La palabra clave **any** puede ser usada en lugar en lugar de destino y comodin-destino.

calificadores-destino son detalles opcionales en el paquete destino, incluyendo numero de puertos y otra información especifica del protocolo.

Log, si esta presente, causa un mensaje acerca del paquete que combina con la regla a ser registrada, y **log-input** causa un mensaje que incluye la interface.

Cisco también ha creado una alternativa llamada *lista de acceso IP nombrada* para las listas de acceso estándar y extendida. Esta función permite referenciar a una lista de acceso por un nombre descriptivo en vez del número. Esto también provee una manera conveniente de construir listas de acceso en línea. La sintaxis para definir una lista de acceso IP por el nombre es mostrado a continuación. Después de que la lista es definida por el nombre, se puede agregar reglas que contengan la palabra clave **permit** o **deny**. Después de la palabra clave **permit** o **deny** la sintaxis es la misma tal como fue definida anteriormente tanto para las listas de acceso estándar o extendida.

ip access-list {**standard|extended**} *name*

Donde

standard especifica una lista de acceso IP estándar

extended especifica una lista de acceso IP extendida.

name es el nombre de la lista de acceso. El nombre no puede contener espacios o puntuación y debe comenzar con un carácter alfabético.

Ejemplos de sintaxis:

El ejemplo que se muestra a continuación muestra como crear una lista de acceso IP extendida pequeña que permite trafico DNS hacia la dirección 14.1.1.2 y cualquier trafico TCP desde el Internet hacia todos los hosts en la red 14.1.0.0/16.

North(config)# **access-list 140 permit udp any host 14.1.1.2 eq 53**

North(config)# **access-list 140 deny udp any any log**

North(config)# **access-list 140 permit tcp any 14.1.0.0 255.255.0.0**

North(config)# **access-list 140 deny ip any any log**

El ejemplo a continuación muestra la misma lista de acceso pero utilizando una lista de acceso IP nombrada:

North(config)# **ip access-list extended border-filter-14**
North(config-ext-nacl)# **permit udp any host 14.1.1.2 eq 53**
North(config-ext-nacl)# **deny udp any any log**
North(config-ext-nacl)# **permit tcp any 14.1.0.0 255.255.0.0**
North(config-ext-nacl)# **deny ip any any log**
North(config-ext-nacl)# **exit**

6.4 FUNCIONES DEL ROUTER

Igualmente importante como proveer interconectividad física para múltiples redes son las funciones lógicas que un router realiza. Estas funciones hacen utilizables las interconexiones físicas. Por ejemplo, comunicaciones interconectadas requieren que por lo menos una vía física interconecte las maquinas origen y destino. Sin embargo, tener y utilizar una vía física son dos cosas diferentes. Especialmente, las maquinas origen y destino deben hablar un mismo lenguaje (*un protocolo enrutado*). Esto también ayuda si los routers yacen entre ellos y también hablan el mismo lenguaje (*un protocolo de enrutamiento*) y acuerdan cual vía física especifica es mejor para usar.

Por lo tanto, algunas de estas funciones que los routers poseen se presentan a continuación:

- Interconectividad física
- Interconectividad lógica
- Cálculo de rutas y mantenimiento

6.4.1 Interconectividad Física

Un router tiene como mínimo dos, y frecuentemente muchos más, puertos físicos de entrada/salida, o *interfaces* como son mayormente conocidos, y usados para conectar físicamente instalaciones de transmisiones hacia el router. Cada puerto esta conectado hacia una tarjeta de circuito que esta conectada hacia la motherboard del router. De esta manera, es la motherboard la que actualmente provee la interconectividad entre las múltiples redes.

El administrador de red debe configurar cada interfaz vía la consola del router. La configuración incluye el definir los números de puerto de las interfaces en el router, la tecnología de transmisión específica y el ancho de banda disponible en la red conectada a esta interfaz, y los tipos de protocolos que serán utilizados a través de esta interfaz. Los parámetros actuales que deben ser definidos varían basados en el tipo de interfaz de red.

6.4.2 Interconectividad Lógica

Tan pronto como la interfaz del router es configurada, esta debe ser activada. La configuración de las interfaces identifica el tipo de instalación de transmisión a la cual se esta conectado, las direcciones IP de las interfaces, y las direcciones de la red a la cual se esta conectado. Con la activación del puerto, el router inmediatamente comienza a monitorear todos los paquetes que están siendo transmitidos en la red conectada con el nuevo puerto activado. Esto permite “aprender” acerca de la red y las direcciones IP de los host que residen en las redes que están siendo alcanzadas vía este puerto. Estas direcciones son almacenadas en tablas llamadas *tablas de enrutamiento*. Las tablas de enrutamiento asocian el numero de puerto de cada interfaz en el router con las direcciones de la capa de red que pueden ser alcanzadas (tanto directa como indirectamente) a través de este puerto.

Un router también puede ser configurado con una *ruta por defecto*. Una ruta por defecto asocia una interfaz de router específica con todas las direcciones de destino desconocidas. Esto permite al router reenviar un datagrama hacia los destinos que

todavía no han sido aprendidos. Las rutas por defecto pueden ser útiles en otras formas también. Las rutas por defecto pueden ser usadas para minimizar el crecimiento de las tablas de enrutamiento.

6.4.3 Cálculo de rutas y mantenimiento

Los routers se comunican unos con otros a través del uso de protocolos predeterminados llamados *protocolos de enrutamiento*, los protocolos de enrutamiento permiten a los routers ser capaces de hacer lo siguiente:

- Identificar las potenciales rutas hacia las redes destino y/o hosts específicos.
- Desarrollar una comparación matemática, conocida como cálculo, para determinar el mejor camino para cada destino.
- Continuamente monitorear la red para detectar cualquier cambio de topología que puede devolver rutas conocidas como rutas inválidas.

Se puedes evaluar los protocolos de enrutamiento a través de numerosos criterios mas específicos que solamente el hecho de evaluar el tipo de aproximación utilizan. Algunos de los criterios más significantes son los siguientes:

- **Optimización:** la optimización describe la capacidad del protocolo de enrutamiento para seleccionar la mejor ruta disponible. Desafortunadamente, la palabra *mejor* es ambigua. Existen muchas maneras diferentes para evaluar las diferentes rutas para cualquier destino. Cada ruta podría resultar en la selección de una ruta "*mejor*" diferente dependiendo del criterio usado. El criterio utilizado por los protocolos de enrutamiento para calcular y evaluar las rutas es conocido como *Métrica de enrutamiento*. Existe una amplia variedad de métricas, y estas varían ampliamente con los protocolos de enrutamiento. Una métrica simple es *la cuenta de saltos (hop count)*, el número de saltos, o routers, que residen entre las máquinas origen y destino.
- **Eficiencia:** otro criterio a considerar cuando se evalúan los protocolos de enrutamiento es la eficiencia operacional. La eficiencia operacional puede ser

medida mediante el examen de los recursos físicos, incluyendo la RAM del router, tiempo del CPU, y el ancho de banda requerido por cualquier protocolo de enrutamiento. Se podría consultar el fabricante del router o el vendedor para determinar las eficiencias relativas de cualquier protocolo que se esta considerando utilizar.

- **Robustez:** un protocolo de enrutamiento debería funcionar de manera confiable en cualquier momento, no solo cuando la red esta estable. Condiciones de error, incluyendo hardware o fallas en las instalaciones de transmisión, errores de configuración de los routers, y aun cargas de tráfico pesado, adversamente afectan la red. Por lo tanto, es crítico que un protocolo de enrutamiento funciones apropiadamente durante los periodos de fallas de la red y/o inestabilidad.
- **Convergencia:** debido a que estos son dispositivos inteligentes, los routers pueden automáticamente detectar cambios en la red. Cuando un cambio es detectado, todos los routers involucrados deben converger en un nuevo acuerdo de la forma de la red y recalcular sus rutas para los correspondientes destinos conocidos. Este proceso de mutuo acuerdo es llamado *convergencia*. Cada protocolo de enrutamiento usa diferentes mecanismos para detectar y comunicar cambios en la red. Por lo tanto, cada uno converge a diferente ritmo. En general, entre mas lento un protocolo de enrutamiento converge, mas grande es el potencial para desorganizar el servicio a través de la red.
- **Escalabilidad:** la escalabilidad de una red es una capacidad para crecer. Aunque el crecimiento no es requerido en cada organización, el protocolo de enrutamiento que se selecciona debería ser capaz de escalar ascendentemente para alcanzar el crecimiento proyectado de la red.
- **Seguridad:** Proveer seguridad es una de las muchas funciones lógicas del router. Asegurar una red que usa un protocolo abierto intencionalmente como lo es el protocolo IP, no es una tarea trivial. El tipo de seguridad que un router puede proveer esta basado en permisos de accesos. Se pueden definir explícitamente permisos por puerto en el router. La lista de permisos es conocida como una *lista de control de acceso - access control list* (ACL).

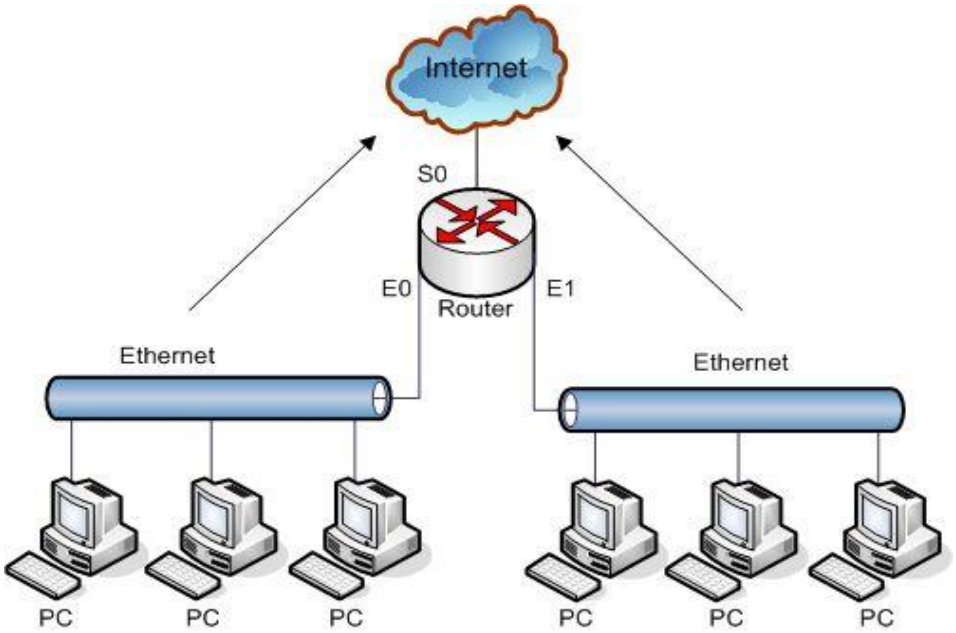


Figura 6.7. Una lista de control de acceso puede reducir el riesgo de internetworking.

6.4.4 Papel del router en las Redes de área Amplia (WAN)

Las redes son caras en términos de cantidad de routers utilizados, instalaciones de transmisión y sistemas finales conectados. En una red extensa como lo es el Internet o aún las redes privadas de grandes dimensiones sería virtualmente imposible para cualquier máquina origen el conocer acerca de la otra máquina destino. Por lo tanto, alguna forma de jerarquía es necesaria. La organización jerárquica de las máquinas interconectadas crea la necesidad para las funciones especializadas del router.

Los routers pueden especializarse tanto en aprender como en distribuir información de enrutamiento hacia los sistemas finales dentro de sus dominios. Estos routers son llamados *entradas interiores (interior gateways)*. Alternativamente, los routers pueden especializarse en recolectar información de enrutamiento acerca de las máquinas que yacen mas allá de su dominio. Estos routers son conocidos como *entradas exteriores (exterior gateways)*.

Networking, es a menudo usado como un término genérico o universal. Sin embargo, las máquinas en una red se comunican de maneras diferentes y de forma muy

efectiva. Los routers pueden funcionar en diferentes capacidades en una red, por ejemplo, como routers interiores, exteriores y de perímetro.

Nota: no es muy raro encontrar routers interiores, exteriores o de perímetro descritos como *gateways interiores, gateways exteriores* o *gateways de perímetro* respectivamente. El termino *gateway* es tan viejo como el enrutamiento mismo. Con el paso de tiempo, este término ha perdido algo de su valor descriptivo. Consecuentemente, ambos conjuntos de términos son técnicamente correctos, excepto en la presencia de puristas tecnológicos. Entonces se tendrá que considerar cual término es considerado correcto.

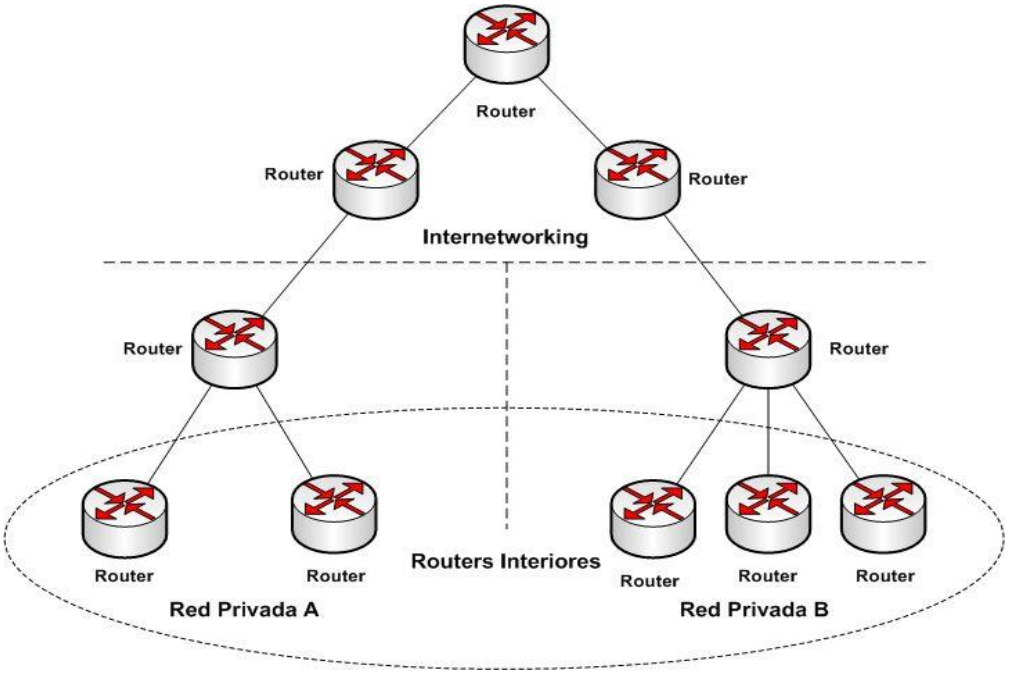


Figura 6.8. Ámbito de los routers interiores

Sistemas autónomos: un sistema autónomo (AS) es una red (tanto LAN como WAN) que esta relativamente auto sostenida. Es administrada por una única persona (o grupo de personas), que presenta un único protocolo enrutado, arquitectura de direccionamiento y usualmente un solo protocolo de enrutamiento. Un sistema autónomo puede soportar conexiones hacia otro sistema autónomo poseído y operado por la misma organización. Alternativamente, un AS puede tener conexiones hacia otras redes, como lo es el Internet, y aun así retiene la autonomía de operación. Este término es usualmente usado en conjunto con protocolos de

enrutamiento específicos, como los es OSPF, que habilita a una red para ser esculpida en numerosas subsecciones.

Dadas estas definiciones, es posible mejor definir las clases funcionales de los routers. Un *router interior* es un router que puede ser usado por sistemas finales en una red para acceder a otros sistemas finales dentro de la misma red. El router interior no soporta conexiones de cualquier otra red. La figura a continuación ilustra una pequeña red y identifica aquellos dispositivos que funcionará como routers interiores.

6.4.5 Routers interiores en una red.

Un router exterior es uno que yace mas allá de los limites de cualquier red. En la figura de las listas de control de acceso, el Internet es descrito como una nube sin rasgos sobresalientes. En la realidad, esta nube tiene una topología específica. En la siguiente figura, aunque no pretendiendo describir la topología actual del Internet, presenta una topología de Internet altamente simplificada que aisladamente pretende demostrar lo que un router exterior es.

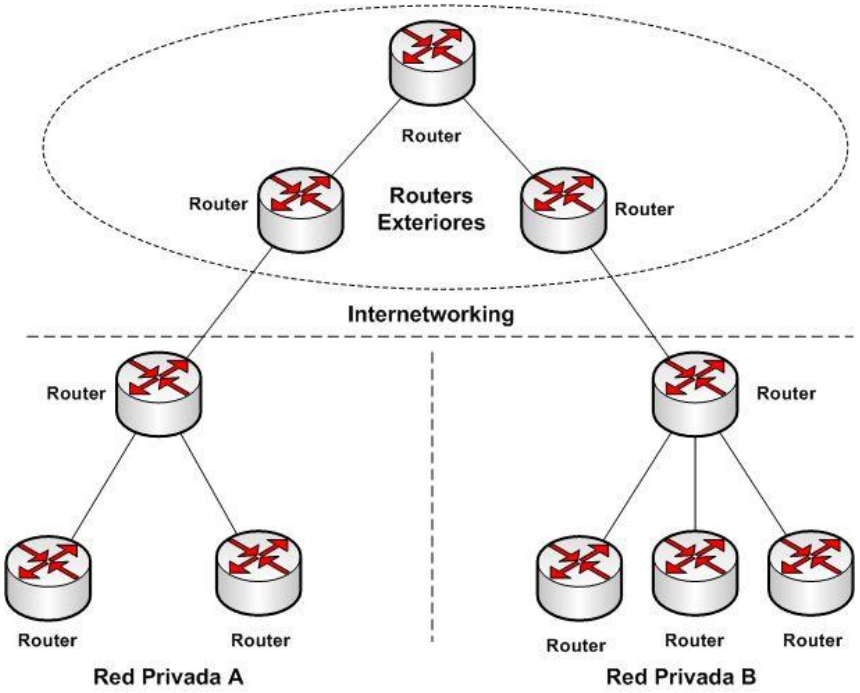


Figura 6.9. Routers exteriores desde la perspectiva de las redes privadas.

La última clase funcional del router es la del router de perímetro. Los routers de perímetro interconectan una red con las otras redes. Es importante notar que una sola entidad puede poseer y operar múltiples sistemas autónomos. Por lo tanto, un router de perímetro puede denotar el límite entre dos sistemas autónomos en lugar del límite entre una red privada y alguna otra red. La siguiente figura, identifica los routers de perímetro en una red de muestra que ha sido usada en las precedentes dos figuras.

6.5. ROUTERS DE PERÍMETRO DESDE LA PERSPECTIVA DE LAS REDES PRIVADAS.

6.5.1 Escenarios de Internetworking.

Habiendo examinado los conceptos fundamentales de enrutamiento y internetworking, así como alguna de la terminología natal de estos temas, ahora se puede ver como estos son utilizados mediante el examen de estos tres escenarios de internetworking. Cada escenario demuestra algunos de los problemas que necesitan ser atendidos en cualquier red o interred:

- Enrutamiento dentro de una red
- Enrutamiento entre redes adyacentes
- Enrutamiento entre redes no adyacentes

Estos tres aspectos genéricos abarcan virtualmente cada forma de internetworking que se puede llegar a encontrar. Cada uno de ellos tiene diferentes implicaciones para el administrador de red, incluyendo aspectos de enrutamiento como el cálculo de ruta, distribución, convergencia y seguridad. La siguiente sección provee un vistazo de cada escenario de internetworking y resalta las áreas de preocupación para un administrador de red. Las variadas soluciones potenciales para estas preocupaciones de enrutamiento están presentadas en esta investigación.

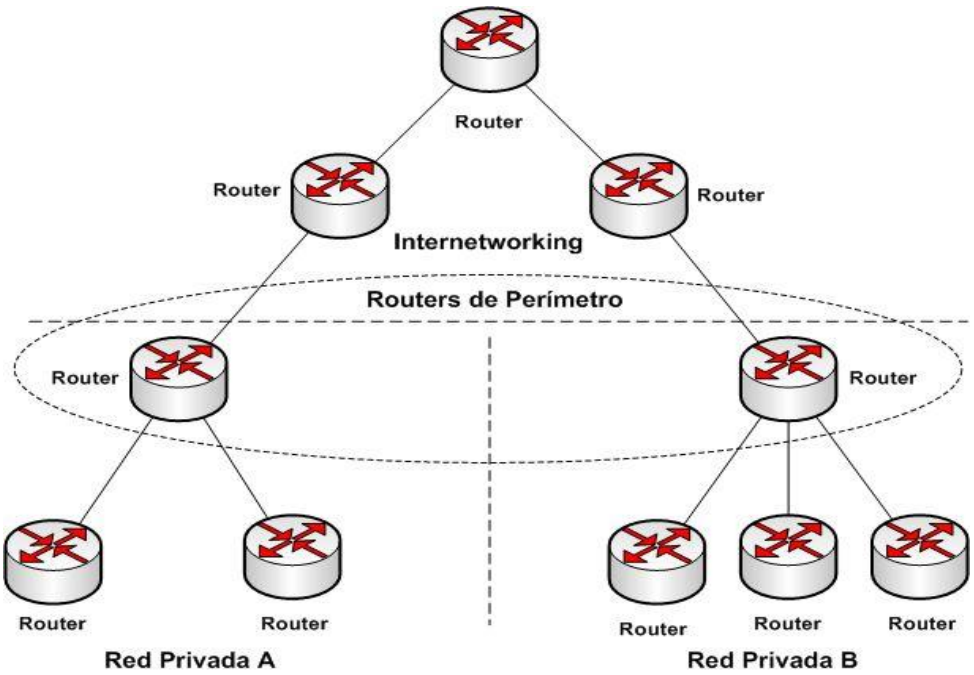


Figura 6.10. Ámbito de los routers de perímetro

6.5.2 Enrutamiento dentro de una red.

La forma mas simple de enrutamiento en el enrutamiento dentro de los confines de una sola red. Esta red consiste solamente de routers interiores. En teoría, esta forma de red usaría solamente un protocolo enrutado, una arquitectura de direccionamiento, y un numero mínimo de destinos. Esto disminuiría grandemente la carga de trabajo de cada router y maximizaría el desempeño de red potencial. Por lo tanto, los problemas de enrutamiento dentro de la Intranet están mas estrechamente relacionados hacia el tamaño de la red y la topología en vez de sus arquitecturas de direccionamiento y protocolos de enrutamiento.

Si la red fuera lo suficientemente pequeña, podría ser factible para el administrador el reprogramar todas las posibles rutas estáticas en vez de introducir la complejidad de un protocolo de enrutamiento dinámico. Las rutas programadas estáticamente, sin embargo, se pueden volver una carga laboriosa con el crecimiento o el constante cambio dentro de la red.

6.5.3 Enrutamiento entre redes adyacentes.

Un pequeño paso mas en la complejidad desde el enrutamiento en la intrared es el enrutamiento de interred entre redes adyacentes. Físicamente adyacentes significa que las dos redes están directamente conectadas el una con la otra. Semejante a una adyacencia que puede haberse diseñado para promover la convergencia rápida, mejorar la seguridad o satisfacer cualquier numero de otros criterios de desempeño.

La separación lógica de las múltiples redes implica que los routers de perímetro entre ellos deben resumir y distribuir la información de enrutamiento entre ellos. De esta manera, los sistemas finales de una red pueden directamente dirigirse hacia los sistemas finales de la otra red, la siguiente figura ilustra este tipo de enrutamiento.

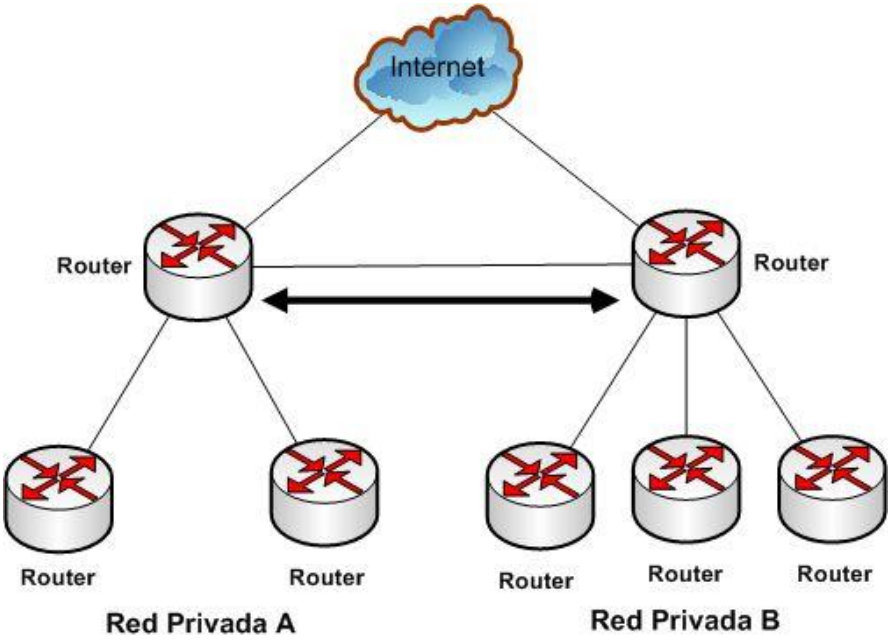


Figura 6.11. Enrutamiento entre redes adyacentes

Los problemas de enrutamiento que necesitan ser atendidos en este tipo de interredes surgen de las diferencias entre las dos redes. Algunas de las diferencias potenciales que deben ser identificadas incluyen lo siguiente:

- Las redes pertenecen a la misma organización? Si no, los routers de perímetro necesitan asegurar sus perímetros de la red.

- Las redes utilizan el mismo protocolo de enrutamiento? Si no, alguna métrica aceptable mutua debe ser encontrada.
- Las redes utilizan el mismo protocolo enrutado? Si no, se tiene que soportar un segundo protocolo enrutado en la red para facilitar la interred.

Adicionalmente, la topología puede afectar el enrutamiento entre redes adyacentes. Usando un punto simple de interconexión entre las dos redes, por ejemplo, hace más fácil el controlar el cálculo y la predistribución de la información de enrutamiento entre las redes. Esta conveniencia introduce un punto simple de fallo, sin embargo, esto puede no ser aceptable para los usuarios. Introduciendo un segundo (o aun mas) puntos de interconexión resuelven el problema del punto simple de falla pero puede crear la oportunidad para que ciclos infinitos de enrutamiento ocurran. Resolver tal dilema requiere un entendimiento de la tolerancia de los usuarios para caídas en la red y riesgos. Equipado con este entendimiento, se pueden evaluar protocolos de enrutamiento específicos y sus capacidades para convertir rápidamente y compensar los problemas potenciales de enrutamiento.

6.5.4 Enrutamiento entre redes no adyacentes:

Enrutamiento entre redes no adyacentes es, simultáneamente, el tipo de enrutamiento mas complicado y a la vez mas utilizado. Las dos redes pueden utilizar una tercera red como un intermediario. Es altamente probable que las tres redes diferentes utilizaran diferentes protocolos de enrutamiento, protocolos enrutados y arquitecturas de direccionamiento. Por lo tanto, el trabajo del router de perímetro es sobrepasar estos obstáculos para la comunicación al mismo tiempo que resguarda el perímetro de su misma red.

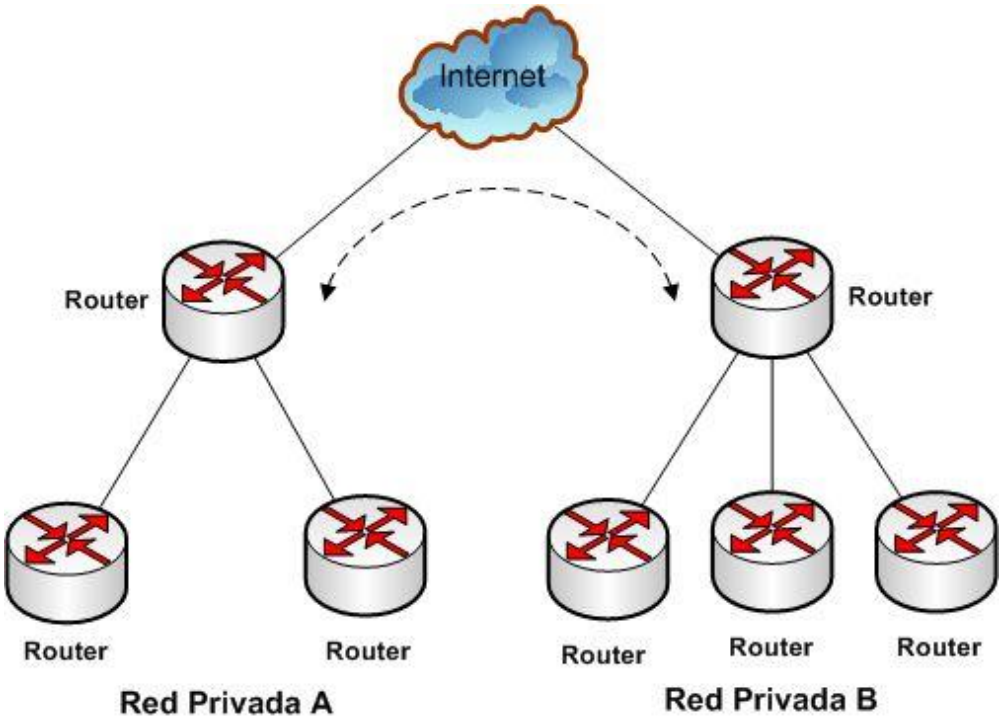


Figura 6.12. Enrutamiento entre redes no adyacentes pequeñas:

El router de perímetro de cada red privada en esta ilustración necesita proteger el perímetro de su propia red de intrusos no deseados. Dado esto, las dos redes que necesitan comunicarse no están adyacente y la red intermediaria esta mas allá de su control, el riesgo de intrusos no deseados es mucho mayor que si estas estuvieran directamente conectadas. Por lo tanto, los administradores de red deben desarrollar un conjunto de criterios para permitir usuarios externos específicos dentro de sus redes, mientras se deshabilita el acceso a todos los demás usuarios. El router de perímetro implementaría estos criterios en una lista de control de acceso (Access Control List-ACL).

Otra responsabilidad para el router de perímetro sería la de resumir las rutas internas y redistribuir esta información hacia las redes externas. Esto permite que usuarios afuera del perímetro de la red privada tener acceso a los sistemas finales de la red. Si esta información de enrutamiento no fuera distribuida, nadie del exterior de la red privada podría tener acceso hacia los sistemas finales.

Finalmente, es altamente probable que los routers de perímetro tengan que ser configurados para utilizar múltiples protocolos de enrutamiento. Un protocolo interior para el router debe ser seleccionado para los propósitos de enrutamiento dentro de la Intranet. El calculo de las rutas a través de la interred, sin embargo, puede requerir un protocolo diferente, uno que desarrolla un soporte fuerte para el resumen de las rutas.

CAPITULO 7. FIREWALLS.

Los firewall son principalmente componentes que brindan seguridad a través del bloqueo de puertos, estos ayudan de gran forma aportando un nivel de seguridad muy alto a la estrategia Defensa en Profundidad. Es necesario saber para que existen, su importancia, como pueden ser utilizados para lograr una mejor seguridad de la red que se quiere proteger, así también conocer las limitantes de un firewall para así no tener una idea de falsa seguridad. No hay que olvidar que los firewall no son perfectos, ya que bloquean lo que se les dice que bloqueen y permiten lo que se les dice que permitan.

Puntos clave:

- Conocer algunas definiciones.
- Comprender porque son importantes.
- Entender el objetivo de un firewall.
- Conocer los peligros que evita un firewall.
- Tipos de firewall.
- Algunas características y requisitos.
- Formas generales en las que se pueden implementar.

Definiciones generales de Firewalls.

Los firewall en general se pueden definir como un dispositivo que funciona como punto de seguridad entre redes, permitiendo o denegando las transmisiones de una red a la otra. Para dar una mejor visión de lo que es un Firewall se tienen las siguientes definiciones.

Firewall: es un sistema diseñado para prevenir el acceso no autorizado hacia y desde una red privada. Los firewall pueden ser implementados en hardware y software, o una combinación de ambos. Los firewall son frecuentemente usados para prevenir a los usuarios sin autorización de acceder a la red privada conectada al Internet. Todos los paquetes que entran o dejan la intranet pasan a través del Firewall, el cual examina cada paquete y bloquea aquellos que no cumplen con los criterios de seguridad especificados.

Firewall: un componente o conjunto de componentes que restringe el acceso entre una red protegida y el Internet o entre otro conjunto de redes.

Otra definición: Firewalls son dispositivos de red de computadoras que protegen una red de otras redes menos confiables, son esencialmente dispositivos de red de control de acceso que permiten o niegan viajar diferente tipo de tráfico hacia dentro o hacia fuera de la red de una organización.

También se definen un firewall como una colección de componentes o sistemas ubicados entre dos redes y que posee las siguientes propiedades:

- Todo el trafico entrante - saliente y viceversa pasa a través de él.
- Solo el trafico autorizado definido por las políticas de seguridad local, esta permitido pasar a través de él.
- El sistema mismo es altamente resistente a la entrada no autorizada.

7.1 PORQUE USAR UN FIREWALL

El Internet, la red global de redes de computadoras que provee la base universal del correo electrónico, el World Wide Web y muchas formas de comercio electrónico, diversamente ha sido descrita casi tan grande como la computadora personal, mas significante que los impresores y tan revolucionaria como el descubrimiento del fuego.

Los Firewalls, los cuáles son diseñados para controlar el flujo de información entre dos redes, se hicieron una realidad aun antes de que el mundo hubiera escuchado acerca de la Internet. El sentido común dice que un administrador debería considerar usar un firewall siempre que conecta dos redes entre si, un proceso llamado: interconexión de redes.

Típicamente, el término del Internet se refiere específicamente al TCP/IP descendiente de la unión de ARPAnet con CSnet en 1982, ahora sirviéndole a decenas de millones de usuarios a través de centenares de miles de máquinas hosts. En casi todos los casos, la interconexión de redes debería considerar el uso de un firewall para monitorear las conexiones de la red. Esto debe de tomarse más en cuenta cuando la interconexión de redes internas incluye una conexión a Internet.

Una reciente encuesta encontró que cuatro de cada cinco organizaciones grandes (de esas con más de 2,500 empleados) corren aplicaciones críticas en redes de área local (LAN). Estas LAN, y la información vital que procesan, progresivamente esta bajo amenaza. Por ejemplo, cuando ICSA estudió un perfil común de 61 organizaciones grandes, encontró 142 violaciones de seguridad en tres meses. IP spoofing, una técnica que puede dar a un hacker acceso extendido para una red interna.

Casi todas las compañías proveen acceso de los empleados a Internet y acceso remoto a redes corporativas, según una encuesta bajo la dirección de la firma de abogados *the Chicagobased information-technology* de Gordon y Glickson. Aún,

menos de la mitad de esas mismas compañías realiza comprobaciones de seguridad de rutina, sólo 44 por ciento tiene la capacidad de rastrear acceso a datos sensibles y sólo una tercera parte usa la encriptación.

Las compañías en la encuesta de Gordon y Glickson, muestran poca atención en su esquema de acceso a Internet. Mientras que desde el punto de vista del 75 por ciento, opinan que les gustaría restringir el acceso a sólo ciertas partes de Internet, sólo 62 por ciento tiene políticas de acceso a Internet, 42 por ciento no monitorea el uso de Internet por parte del empleado y sólo 30 por ciento realmente aplica controles de acceso. Además, menos de dos a cinco encuestados imponen restricciones en hacer una descarga de archivos de terceros, es admirable que solo uno de seis reportó estar experimentando un efecto negativo asociado con el uso de Internet por empleados y una de ocho reportan reclamos legales proviniendo del uso de tecnologías de información por parte de un empleado.

Muchas organizaciones aún temen aprovecharse de las virtudes que brinda Internet, por los riesgos que esto implica. Para superar estos temores y proveer el nivel de protección requerida, las organizaciones necesitan seguir una política de seguridad para prevenir accesos indebidos a los recursos de la red privada y protegerse contra la fuga de información. La pregunta hoy, no es si las organizaciones deben entrar en el mundo de Internet e incorporar la tecnología de información y las comunicaciones en sus procesos productivos, sino cómo utilizarlas para mejorar la calidad del trabajo, para mantener un alto grado de competitividad y para contribuir al logro de sus objetivos principales, en un ambiente de control “confiable”.

El Internet ha crecido para asumir todos los demás problemas de seguridad de red, incluyendo a los virus, los caballos de Troya y violación de redes internas. Una red conectada a Internet conlleva un conjunto de nuevos riesgos, una cierta cantidad de los cuales agrava los problemas existentes. Las organizaciones cuyas redes permanecen desconectadas de Internet reciben presión para hacer esa conexión, simplemente para el correo electrónico. La presión a menudo se hace tan fuerte, que

algunos departamentos o usuarios individuales se conectan a Internet sin el conocimiento y la debida autorización de la gerencia.
Al fin de cuentas cuando una compañía conecta su red a otra red, cosas malas pueden ocurrir. Si la compañía quiere protegerse y monitorear esas cosas malas, necesita poner una fuerte combinación de políticas y tecnologías de seguridad en el lugar.

7.1.1 Protección de la red

Los Firewalls entran en el cuadro cuando una organización desconfía de cualquier red interconectada. Siempre se debería desconfiar del Internet, pero la experiencia nos dice en realidad que no deberíamos confiar en cualquier red, aun aquellas dentro de nuestra compañía, a menos que tengamos completa seguridad de su estatus de seguridad. En otras palabras, alguien responsable por las ventas de la compañía y la red de mercadeo no puede asumir que la producción de la compañía y la red de inventario son confiables, a menos no sin alguna clase de seguridad medianamente fuerte.

7.1.2 Objetivo básico de un Firewall.

En pocas palabras, un firewall lleva a cabo tres funciones para proteger su red:

- Bloquea los datos entrantes que pueden contener el ataque de un “hacker”.
- Oculta la información acerca de la red, haciendo que todo parezca como si el tráfico de salida se originara del firewall y no de la red. Esto también se conoce como NAT (Network Address Translation).
- Filtra el tráfico de salida, con el fin de restringir el uso de Internet y el acceso a localidades remotas.

7.1.3 Tipos de peligros que puede evitar un firewall

- Instalación y ejecución de programas instalados clandestinamente desde Internet, por ejemplo vía aplicaciones ActiveX o Java que pueden llegar a transferir datos personales del usuario a sitios.
- Acceso de terceros por fallas o errores de configuración de Windows (por ejemplo de NetBIOS).
- Instalación de publicidad (advertisers) o elementos de seguimiento (track) como las cookies.
- Troyanos: aplicaciones ocultas que se descargan de la red y que pueden ser usadas por terceros para extraer datos personales. A diferencia del virus, estos troyanos son activados en forma remota por un tercero.
- Reducción del ancho de banda disponible por el tráfico de banners, pop ups, sitios no solicitados, y otro tipo de datos innecesarios que ralentizan la conexión.
- Spyware.
- Utilización de la línea telefónica por terceros por medio de Dialers (programas que cortan la actual conexión y utilizan la línea para llamadas de larga distancia)

7.2 VENTAJAS Y DESVENTAJAS DE LOS FIREWALL

7.2.1 Ventajas

- Los firewalls en Internet administran los accesos posibles del Internet a la red privada. Sin un firewall, cada uno de los servidores propios del sistema se expone al ataque de otros servidores en el Internet. Esto significa que la seguridad en la red privada depende de la "Dureza" con que cada uno de los servidores cuenta y es únicamente seguro tanto como la seguridad en la fragilidad posible del sistema.
- El firewall permite al administrador de la red definir un "choke point" (embudo), manteniendo al margen los usuarios no-autorizados (tal, como., hackers, crakers, vándalos, y espías) fuera de la red, prohibiendo potencialmente la

entrada o salida al vulnerar los servicios de la red, y proporcionar la protección para varios tipos de ataques posibles. Uno de los beneficios clave de un firewall en Internet es que ayuda a simplificar los trabajos de administración, una vez que se consolida la seguridad en el sistema firewall, es mejor que distribuirla en cada uno de los servidores que integran nuestra red privada.

- El firewall ofrece un punto donde la seguridad puede ser monitoreada y si aparece alguna actividad sospechosa, este generara una alarma ante la posibilidad de que ocurra un ataque, o suceda algún problema en el transito de los datos. Esto se podrá notar al acceder la organización al Internet, la pregunta general es "si" pero "cuando" ocurrirá el ataque. Esto es extremadamente importante para que el administrador audite y lleve una bitácora del tráfico significativo a través del firewall. También, si el administrador de la red toma el tiempo para responder una alarma y examina regularmente los registros de base. Esto es innecesario para el firewall, desde que el administrador de red desconoce si ha sido exitosamente atacado.
    - Concentra la seguridad Centraliza los accesos.
    - Genera alarmas de seguridad Traduce direcciones (NAT)
    - Monitorea y registra el uso de Servicios de WWW y FTP.

Firewall de Internet.

Con el paso de algunos años, el Internet ha experimentado una crisis en las direcciones, logrando que el direccionamiento IP sea menos generoso en los recursos que proporciona. Por este medio se organizan las compañías conectadas al Internet, debido a esto hoy no es posible obtener suficientes registros de direcciones IP para responder a la población de usuarios en demanda de los servicios. Un firewall es un lugar lógico para desplegar un Traductor de Direcciones de Red (NAT) esto puede ayudar aliviando el espacio de direccionamiento acortando y eliminando lo necesario para re-enumerar cuando la organización cambie del Proveedor de Servicios de Internet (ISP).

Un firewall de Internet es el punto perfecto para auditar o registrar el uso del Internet. Esto permite al administrador de red justificar el gasto que implica la conexión al

Internet, localizando con precisión los cuellos de botella potenciales del ancho de banda, y promueve el método de cargo a los departamentos dentro del modelo de finanzas de la organización.

Un firewall de Internet ofrece un punto de reunión para la organización. Si una de sus metas es proporcionar y entregar servicios información a consumidores, el firewall de Internet es ideal para desplegar servidores WWW y FTP.

Finalmente, el firewall puede presentar los problemas que genera un punto de falla simple. Enfatizando si este punto de falla se presenta en la conexión al Internet, aun así la red interna de la organización puede seguir operando, únicamente el acceso al Internet esta perdido - .

La preocupación principal del administrador de red, son los múltiples accesos al Internet, que se pueden registrar con un monitor y un firewall en cada punto de acceso que posee la organización hacia el Internet. Estos dos puntos de acceso significan dos puntos potenciales de ataque a la red interna que tendrán que ser monitoreados regularmente.

7.2.2 Desventajas.

- Un firewall no puede protegerse contra aquellos ataques que se efectúen fuera de su punto de operación.
- El firewall no puede protegerse de las amenazas a que esta sometido por traidores o usuarios inconscientes. El firewall no puede prohibir que los traidores o espías corporativos copien datos sensitivos en disquetes o tarjetas PCMCIA y substraigan estas del edificio.
- El firewall no puede proteger contra los ataques de la "Ingeniería Social". Para controlar estas situaciones, los empleados deberían ser educados acerca de los varios tipos de ataque social que pueden suceder, y a cambiar sus contraseñas si es necesario periódicamente.

- El firewall no puede proteger contra los ataques posibles a la red interna por virus informativos a través de archivos y software, obtenidos de Internet al momento de comprimir o descomprimir archivos binarios, el firewall de Internet no puede contar con un sistema preciso de SCAN para cada tipo de virus que se puedan presentar en los archivos que pasan a través de él.

  La organización debe ser consciente en instalar software antivirus en cada computadora para protegerse de los virus que llegan por medio de disquetes o cualquier otra fuente.
- Finalmente, el firewall de Internet no puede proteger contra los ataques posibles en la transferencia de datos. Estos ocurren cuando aparentemente datos inocuos son enviados o copiados a un servidor interno y son ejecutados facilitando un ataque.
- Los Firewalls no maneja ataques internos, ya que proveen defensa sólo del perímetro. Firewalls no son sistemas de control de acceso multiuso y no controlan el abuso de personas de confianza de acceso autorizado, quizá el máximo riesgo de todos.

Las encuestas de protección de la información reportan que la mitad de los incidentes son ataques internos, y muchos profesionales de seguridad creen que los ataques internos dan lugar hasta 80 por ciento de todos los problemas de seguridad. Otro problema grande es que los Firewall no protegen de código malicioso, virus y caballos de Troya. Los virus son código auto generativo que puede causar interrupción considerable en redes tan bien como en las estaciones de trabajo individuales. Un programa caballo de Troya, finge ser algo que no es, logrando las metas de su creador. El problema se extiende a todas las organizaciones que están conectadas a la red pública.

El código malicioso ahora viaja más rápido que antes, en particular nuevos tipos de virus que usan idiomas de macro para esparcir a través de compartir documentos en lugar de programas. Pueden viajar por la Red o a través de la Web como anexos por correo electrónico. El Internet mismo es una fuente de programas invasores y destructivos, lo cual puede ser descargado de un cierto número de sitios. Más allá las

cosas se complican, muchos usuarios envían sus programas por correo electrónico o sus sistemas operativos carga e interpretan envíos por correo electrónico, adjuntos como documentos de Word o los documentos HTML sin escanear si hay virus.

Internet también ofrece un camino potencial para caballos de Troya, un problema potencialmente serio para las tecnologías de aplicación distribuida como Java y ActiveX.

Firewalls sólo pueden direccionar código malicioso viniendo de otra red, pero muchas infecciones de virus ocurren cuando las personas se introducen directamente en la red o a los sistemas con discos infectados. Cuando un vendedor ambulante, por ejemplo, regresa con una computadora portátil infectada y la adjunta a la red, el virus puede infectar el sistema entero. Los ingenieros de mantenimiento ocasionalmente introducen discos infectados al sistema durante experimentos.

7.3 TIPOS DE FIREWALL

7.3.1 Filtros estáticos a nivel de paquete (Static Packet Filters):

Esta tecnología pertenece a la primera generación de firewalls la cual analiza el tráfico de la red. Cada paquete que entra o sale de la red es inspeccionado y lo acepta o rechaza basándose en las reglas definidas por el usuario. El filtrado de paquetes es efectivo y transparente para los usuarios de la red, pero es difícil de configurar. Además de que es susceptible a IP Spoofing.

Se basa en permitir o denegar el tráfico basado en el encabezado de cada paquete. Como no guarda los estados de una conexión, es decir no tiene el concepto de una sesión.

Este tipo de implementación era popular antes de la aparición de los Firewalls y aun se encuentra ya que normalmente hace parte del sistema operativo (Linux o Windows)

Por lo anterior no puede reconocer un ataque o evitar un DoS (Denial of Service). La mayoría de dispositivos pequeños o enrutadores para el hogar o SOHO, incluso los enrutadores CISCO viene con la tecnología de filtrado de paquetes.

Las reglas para rechazar o aceptar un paquete son las siguientes:

- Si no se encuentra una regla que aplicar al paquete, el paquete es rechazado.
- Si se encuentra una regla que aplicar al paquete, y la regla permite el paso, se establece la comunicación.
- Si se encuentra una regla que aplicar al paquete, y la regla rechaza el paso, el paquete es rechazado.
- Se basa en las direcciones de origen y destino.
- Puede utilizar el protocolo y/o puertos de origen y destino.

Ventajas

- Eficiencia.
- Fácil implementación

Desventajas

- Complejidad de las reglas.
- No ofrece autenticación.
- Vulnerable a ataques como Spoofing (cambio de dirección del remitente).
- Difícil de administrar en ambientes complejos.

7.3.2 Firewall a nivel de circuito (Circuit Level Firewalls):

Esta tecnología pertenece a la segunda generación de firewalls y valida que los paquetes pertenezcan ya sea a una solicitud de conexión o bien a una conexión entre dos computadoras. Aplica mecanismos de seguridad cuando una conexión TCP o UDP es establecida. Una vez que la conexión se establece, los paquetes pueden ir y venir entre las computadoras sin tener que ser revisados cada vez.

El firewall mantiene una tabla de conexiones válidas y permite que los paquetes de la red pasen a través de ella si corresponden a algún registro de la tabla. Una vez terminada la conexión, la tabla se borra y la transmisión de información entre las dos computadoras se cierra.

7.3.3 Firewall a nivel de aplicación (Application Layer Firewalls).

Pertenece a la tercera generación de firewalls. Examina la información de todos los paquetes de la red y mantiene el estado de la conexión y la secuencia de la información. En este tipo de tecnología también se puede validar claves de acceso y algunos tipos de solicitudes de servicios.

La mayoría de estos tipos de firewalls requieren software especializado y servicios Proxy. Un Servicio Proxy es un programa que aplica mecanismos de seguridad a ciertas aplicaciones, tales como FTP o HTTP. Un servicio proxy puede incrementar el control al acceso, realizar chequeos detallados a los datos y generar auditorias sobre la información que se transmite.

7.3.4 Filtros dinámicos a nivel de paquete (Dynamic Packet Filters).

Pertenece a la cuarta generación de firewall y permite modificaciones a las reglas de seguridad sobre la marcha. En la práctica, se utilizan dos o más técnicas para configurar el firewall. Un firewall es considerado la primera línea de defensa para proteger la información privada.
Características.

- Genera reglas automáticamente
- Facilita el manejo respecto la versión estática

Ventajas:

- Facilita la administración
- más “exactitud” en el filtrado

7.3.5 Firewall Proxy (Circuit Gateways)

En este caso la pasarela actúa del mismo modo que un simple cable (vía Software) conectando la red interna con el exterior. En general se requiere que el usuario esté autorizado para acceder al exterior o interior y que tenga una cuenta de salida en el proxy.

Son “proxys” no inteligentes.

- Simplemente reenvían la conexión.
- El cliente debe conocerlo.
- Es independiente del protocolo.
- Se usan en combinación con políticas estrictas de filtrado.

Desventajas.

- Ciertos sistemas como SOCKS necesitan programas cliente modificado para soportarlo.

7.3.6 Gateways de aplicación.

Para contrarrestar una cierta cantidad de las debilidades asociadas con los routers de filtrado de paquetes, los desarrolladores han creado programas de aplicación que reenvían y filtran conexiones de servicios como TELNET y el FTP. Tales aplicaciones son llamadas servidores proxy, también conocido como gateways de aplicación. Máquinas hosts corriendo el servidor proxy son llamados firewalls del gateway de aplicación. Trabajando en conjunto, los firewalls del gateway de aplicación y routers de filtrado de paquetes potencialmente pueden proveer niveles más altos de seguridad y flexibilidad que ellos solos.

Firewalls del gateway de aplicación sólo permiten pasar aquellos servicios que tienen un servidor Proxy, en otras palabras, si un gateway de aplicación contiene proxies para FTP y TELNET, entonces sólo FTP y TELNET pueden estar permitidos en la

subred protegida y todos los demás servicios están completamente bloqueados. Para algunos sitios, este grado de seguridad es importante, ya que garantiza que sólo aquellos servicios que se consideran confiables son admitidos a través del firewall. También impide otros servicios no confiables de ser implementados a espaldas de los administradores del firewall.

Los gateways de aplicación le ofrecen un número de ventajas generales sobre el modo predeterminado de aceptación de tráfico aplicativo directamente para los host internos. Estas ventajas incluyen:

- **Ocultar información**. Los nombres de sistemas internos no necesitan necesariamente ser resueltos por el DNS para los sistemas exteriores, ya que el gateway de aplicación puede ser el único host cuyo nombre debe resolverse a los sistemas exteriores.
- **Logging y autenticación robusta.** El gateway puede autenticar tráfico aplicativo antes de que alcance a los hosts internos. El tráfico luego puede ser puesto en bitácora más eficazmente que con estándar host logging.
- **La eficacia de costos.** El hardware o software de terceros para la autenticación o la necesidad de logging se halla sólo en el gateway de aplicacion.
- **Regals de filtración menos complicadas.** Las reglas en el router de filtrado de paquetes estarán menos complicadas de lo que estarían si el router necesitase filtrar tráfico aplicativo y dirigirlo a un número de sistemas específicos. El router necesita permitir sólo tráfico aplicativo destinado a el gateway de aplicación y niega el resto.

7.3.7 Inspección de Paquetes.

Algunos firewalls de Internet combinan las ventajas de filtrado de paquetes y gateway de aplicación, usando computadoras para filtrar paquetes o routers para controlar la comunicación a capas mas bajas. Esto puede crear un alto grado de control de acceso. Sin embargo, esta configuración puede colocar límites en transparencia,

flexibilidad y conectividad, también puede ser caro en términos de implementación del esquema, administración y técnica. Otra forma de ganar aceptación es inspeccionar paquetes en vez de simplemente el filtrado de ellos; es decir, para considerar su contenido así como también sus direcciones. Firewalls de este tipo emplean un módulo de inspección, aplicable para todos los protocolos, Esta estrategia puede proveer seguridad de sensibilidad al contexto para aplicaciones complejas y puede ser más efectiva que tecnologías que sólo pueden acceder a los datos en ciertas capas.

También tienen en cuenta al estado de las conexiones que maneja a fin de que, por ejemplo, un paquete entrante legítimo pueda ser comparado con la petición del exterior de ese paquete y puede permitirse que entre. Inversamente, un paquete entrante enmascarándose como una respuesta para una petición del exterior inexistente puede ser bloqueado.

El módulo de inspección usa las comunicaciones previas para derivar al estado de la comunicación actual que esta siendo intentada. El filtrado inteligente puede eficazmente combinarse con la habilidad de hacer rastreo de sesión de red, para usar información acerca del comienzo y final de sesiones en decisiones filtrantes. Esto es conocido como la sesión de filtración. El filtro usa reglas hábiles, así mejorando el proceso filtrante y controlando la sesión de red en vez de controlar los paquetes individuales.

7.4 REQUISITOS BÁSICOS.

Las características exactas de las necesidades de los firewall para poder eficazmente implementar las políticas específicas de una organización varía en general, sin embargo, un firewall debería poder hacer lo siguiente:

- Soporte para “denegar todos los servicios excepto aquellos específicamente permitidos”.
- Soporte para políticas de seguridad.

- Adecuar necesidades y servicios nuevos si las normas de actuación sobre seguridad de la organización cambian.
- Incluir medidas avanzadas de autenticación o los medios para instalar medidas avanzadas de autenticación si es necesario.
- Emplear técnicas para permitir o negar los servicios a sistemas específicos según se necesite.
- Log de acceso hacia y a través del firewall.
- Uso de un lenguaje flexible, de fácil manejo de IP-FILTER que sea fácil de programar y que pueda filtrar en una variedad grande de atributos, incluyendo la dirección IP del origen y destino, tipo de protocolo, puerto TCP/UDP origen y destino y la interfaz de entrada y salida.
- Si los usuarios requieren servicios como NNTP, X11, http o gopher, el firewall lo haría bien para soportar los servicios correspondientes. El firewall típicamente también debería actuar como un gateway de correo para el correo del Internet, reduciendo conexiones SMTP entre sitio y los sistemas remotos. Esto da como resultado manejo centralizado de correo electrónico del sitio.
- El firewall debería permitir el acceso público al sitio, algo semejante a que el firewall puede proteger información de servidores públicos mientras los separa de otros sistemas que no requieren que el público tenga acceso.

7.5 REQUISITOS ADICIONALES

El firewall debe poder concentrar y filtrar acceso dial-in. Debe contener mecanismos para poner en logs el tráfico y actividad sospechosa, así como mecanismos para la reducción de logs para mantener los logs legibles y comprensibles. Si el firewall requiere un sistema operativo como UNIX, una versión segura del sistema operativo debería ser incluido, junto con otras herramientas de seguridad necesarias para asegurar la integridad del host del firewall, y todos los parches de sistema operativos instalados.

No hay razón por la cual la máquina firewall tenga el mismo sistema operativo que la red de la compañía. Ciertamente, los numerosos firewalls usan su sistema operativo

propietario, optimizados para la actuación y la seguridad. Sin embargo, operar el firewall puede ser más simple en un sistema con un sistema operativo conocido y que se pueda interactuar fácilmente.

La fuerza del firewall y la exactitud debe ser verificable. Su diseño debe ser simple a fin de que los administradores lo puedan entender y lo puedan mantener. El firewall y cualquier sistema operativo correspondiente debe estar actualizados con parches y otros bugs fixes en el momento indicado.

El Internet cambia constantemente, nuevas vulnerabilidades pueden aparecer, nuevos servicios y mejoras a otros servicios pueden representar dificultades potenciales para cualquier instalación de firewall. Además, la flexibilidad para adaptar a necesidades cambiantes es importante, como lo es el proceso de estar al corriente de vulnerabilidades y problemas. Se recomienda suscribirse a una compañía o asociación que le comunique los nuevos problemas y vulnerabilidades que van apareciendo.

7.6 CARACTERÍSTICAS RELEVANTES EN EL FIREWALL

Importante al escoger un firewall.

Primero determinar el número de usuarios de la organización y su sensibilidad. Para una empresa pequeña de menos de 25 usuarios uno sencillo de packet filtering debería ser suficiente.
Pero si esta misma empresa maneja información sensible o tiene usuarios externos sobre la VPN, debería pensar en un Firewall más sofisticado y mirar la lista siguiente:

- Que tipo de firewal es y si soporta nivel de aplicación
- Que ancho de banda es capaz de manejar en cada uno de los modos de operación (Statefull y Full inspection)
- Que tan fácil de administrar es, posee consola para administración segura, remota y cifrada?

- Que tipos de protocolos de autenticación maneja (RSA, RADIUS, 802.1x etc.)
- Cuantos puertos de LAN independientes tiene (1, 2, 3) y con que velocidad cada puerto (esto para crear zonas des militarizadas DMZ o para segmentar la red interna)
- Tiene facilidad de integrar control de Contenido en navegación?
- Tiene facilidad de integrar control Antivirus en ftp y http?
- Es capaz de comportarse como Transparent Proxy?
- Experiencia del fabricante y del Proveedor específica en temas de seguridad y cortafuegos.
- Sobre que plataforma corre el firewall, si es sobre un sistema operativo propietario o sobre sistema operativo de amplia distribución.
- Es importante que tenga Integración con el Directorio Activo, LDAP u otros sistemas de creación de usuarios.
- ¿Tiene la opción de un sistema de tolerancia a fallas o balanceo de cargas?
- ¿Posee IDS o detección de intrusos en tiempo Real?

7.7. ESQUEMAS DE REDES CON FIREWALL.

7.7.1 Screening Router

- Filtra paquetes
- Reglas complejas
- Poca inteligencia Generalmente asociado a filtrado estático

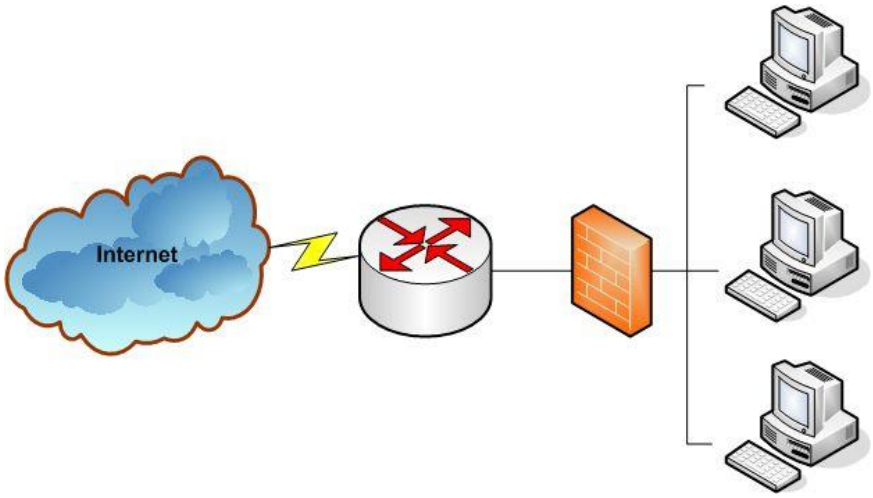


Figura 7.1. Screening Router

7.7.2 Screened Host (Bastion Host)

- Solo permite paquetes al bastion host
- Reglas más simples
- El BH debe ser seguro
- Suele tener Proxies

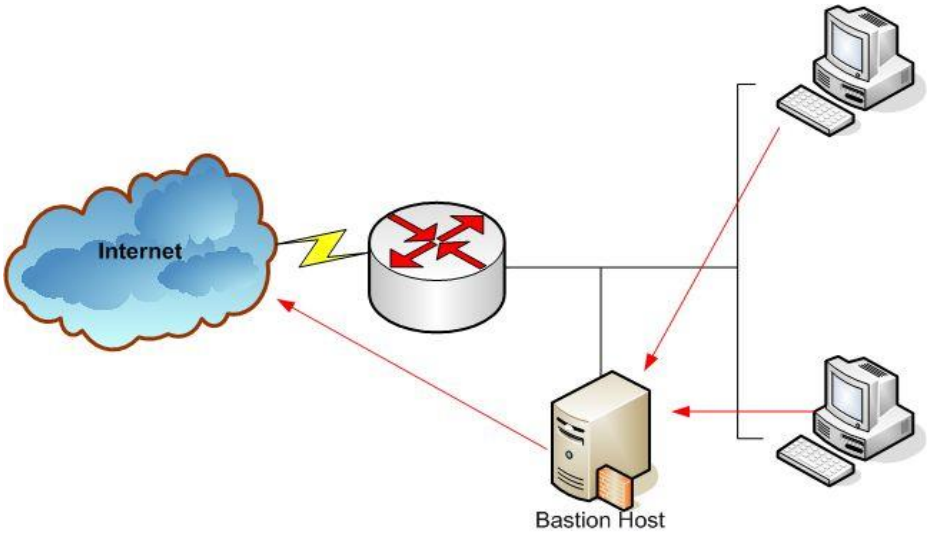


Figura 7.2. Screened Host (Bastion Host)

7.7.3 Screened Host (Dual homed Bastion Host)

- Sin ruteo a través del BH
- BH con Proxies
- Muy Robusto
- El BH debe ser seguro

- No se necesita NAT

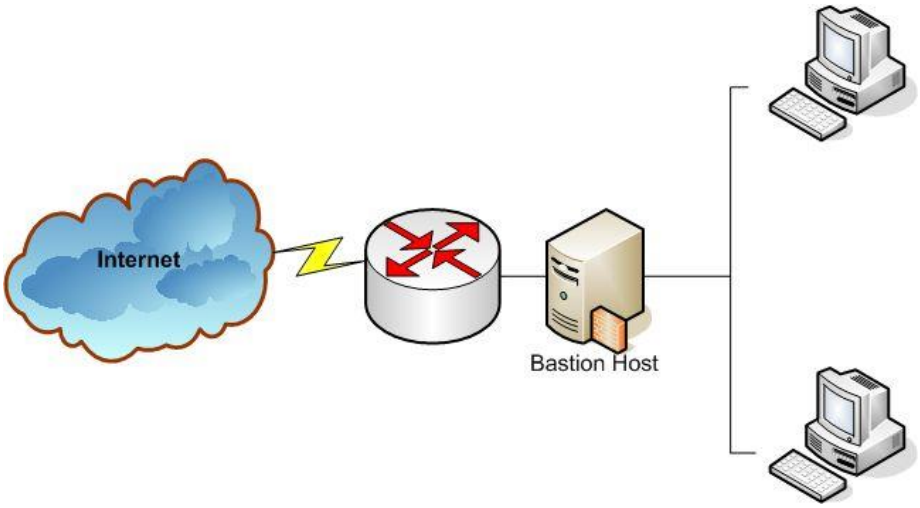


Figura 7.3. Screened Host (Dual homed Bastion Host)

7.7.4 Firewall con DMZ.

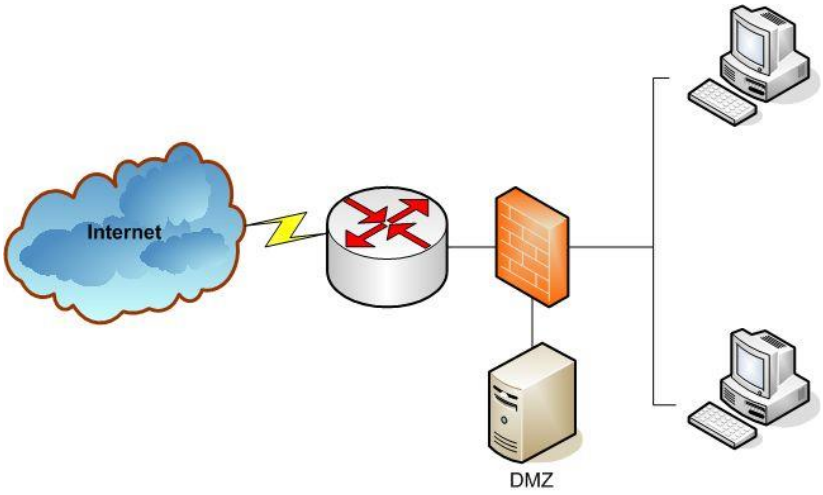


Figura 7.4. Firewall con DMZ.

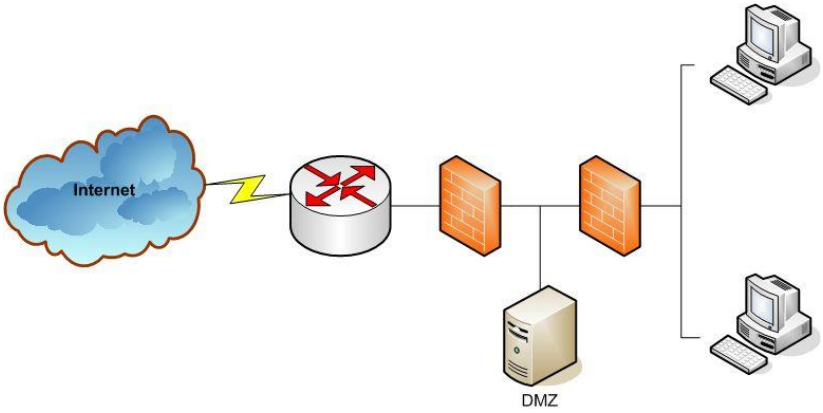


Figura 7.5. Firewall con DMZ.

7.8. METODOLOGÍA PARA SELECCIÓN E INSTALACIÓN DE FIREWALLS

7.8.1. Preselección del Producto

La mayoría de los firewalls emplean una combinación de técnicas para llevar a cabo su labor de la forma más eficiente y segura.

El filtrado de paquetes, la utilización de servidores proxy y la traducción de direcciones de red (NAT) son, en la actualidad, las técnicas más utilizadas.

Algunos protocolos, como por ejemplo Telnet y SNMP, se pueden manejar con más efectividad con filtrado de paquetes. Otros (como FTP o HTTP) se manejan con más efectividad con servidores proxy.

El firewall debe poder configurarse para bloquear todo tipo de tráfico entrante o saliente, excepto para algunos servicios, tales como:

1. TELNET
2. FTP
3. HTTP
4. HTTPS
5. SMTP
6. DNS

TELNET, en el puerto 23, a menudo se permite sólo a algunos sistemas. Igualmente FTP, en los puertos 20 y 21, se permite sólo a algunos sistemas. SMTP, en el puerto 25, se permite sólo a algunos servidores de correo centrales. DNS, en el puerto 53, proporciona información sobre los hosts y que pudiera ser útil para un atacante.

Los siguientes servicios son inherentemente vulnerables y no deberían autorizarse:

- TFTP (Trivial FTP)
- X Windows, en los puertos arriba de 6000

- RPC (Remote Procedure Call) en el puerto 111
- Rlogin, rsh y rexec, en los puertos 513, 514 y 512

El firewall debe permitir llevar un registro de todos los eventos y en particular de todos los accesos permitidos, así como de todos los intentos de acceso fallidos.

El firewall debe poseer un sistema de gestión local y remota para facilitar su configuración y elaborar reportes de auditoria. Las sesiones de administración deben realizarse encriptadas y se requiere un mecanismo de autenticación robusto para tener acceso al firewall.

7.8.2. Análisis de costos

Estos son algunos de los costos que se tienen que considerar al momento de adquirir un dispositivo firewall.

Costos no recurrentes

- Hardware
- Software
- Adiestramiento
- Certificados digitales, tokens, tarjetas inteligentes
- Otros

Costos recurrentes

- Sueldos del personal a cargo del firewall
- Honorarios de consultores externos
- Mantenimiento
- Seguro
- Actualizaciones y parches
- Auditoria
- Otros

7.9. CLASIFICACIÓN DE FIREWALL

7.9.1. Firewall basado en Software

La siguiente tabla contiene algunas soluciones basadas en software.

PRODUCTO	Compañia
Trend Micro PC-cillin Internet Security 2005	Trend Micro™
ZoneAlarm Pro firewall	Zone Labs Inc.
Norton Internet Security 2005	Symantec
Sygate Personal Firewall	Sygate, Inc.
McAfee Internet Security	McAfee, Inc.
Astaro	Astaro
BorderManager	Novell
CyberGuard Premium Firewall Appliance Line	CyberGuard Corporation
eTrust Firewall on Windows 2000	Computer Associates
EdgeForce Family of Security Gateways	ServGate Technologies
FortiGate Family of Antivirus Firewalls	Fortinet Inc.
FutureSoft Firewall	Future Software
Internet Security and Acceleration Server 2000	Microsoft
StoneGate	Stonesoft Corporation
WinRoute Firewall	Kerio Technologies Inc.

Tabla 7.1. Soluciones de Firewall basadas en Software.

7.9.2. Firewall basado en Hardware.

La siguiente tabla contiene algunas soluciones basadas en software.

Equipo	Compañia	Recomendado Para
5000 Series Switch Firewall	Aruba Wireless Networks	Corporación
Alteon Switched Firewall Family	Nortel Networks	Corporación
Cable\DSL Prosafe Firewall FR114P	Netgear	Residencial
ProSafe VPN Firewall family		Pequeña/mediana empresa

CableMedea Firewall	Broadcom	Residencial
Cayman 3300-ENT Series Product Family	Netopia	Residencial
Check Point Next Generation FireWall-1 Linux	Check Point Software	Corporación
Cisco PIX Firewall Family	Cisco Systems, Inc.	Corporación
Cisco IOS Router Firewall Family	Cisco Systems, Inc.	Corporación
GreatSpeed GS-1540G	RIAS Corporation	Residencial
GTA Firewall Family	Global Technology Associates, Inc.	Corporación
iGateway	Intoto, Inc.	Corporación
Inkra 4000 Virtual Service Switch	Inkra Networks	Corporación
IPS-Firewalls Product Family	Netasq	Corporación
Lucent VPN Firewall Family	Lucent Technologies	Corporación
M-Series Router Family	Juniper Networks	Corporación
NC-1000 Series Web Security Gateway	NetContinuum	Corporación
NetScreen Family	NetScreen Technologies	Corporación
Proventia M Series Integrated Security Appliance Family	Internet Security Systems, Inc.	Corporación
RN5C	Ranch Networks	Corporación
SnapGear SME550	SnapGear Inc.	Pequeña/mediana empresa
TZ170	SonicWALL	Pequeña/mediana empresa
VarioSecure	VarioSecure Networks	Corporación
Vigor 2900	Draytek Corporation	Pequeña/mediana empresa
WatchGuard Firebox System Family	WatchGuard	Pequeña/mediana empresa
WatchGuard Firebox Vclass Family	WatchGuard	Corporación
WolfPac Security Platform SG2020	NetWolves Technologies	Corporación

Tabla 7.2. Soluciones de Firewall basadas en Hardware.

7.9.3. Características de Firewalls comerciales.

a. BlackIce

Cuenta con varios niveles de protección y cuando somos escaneados nos avisa mediante un sonido y un icono parpadeante. Ofrece una cantidad de información

sobre los atacantes y estadísticas seguidas de los ataques, detalladas por horas, días y meses.

b. Conseal PC

Está un poco desfasado y tiende a su desaparición, al instalarse copia varios ficheros antiguos, pero Windows te advierte, y se restauran las versiones antiguas que ha copiado por las más recientes que tengas en tu ordenador.

c. Terminet

Es de idioma español. Además de que es muy fácil de usar, no es necesario cambiar la configuración por defecto para poder gozar de una buena protección.

d. Tiny

Viene configurado con un nivel de seguridad medio, conveniente para una navegación normal en Internet. Muestra cerrados algunos puertos y en modo invisible otros. En la red trabaja muy bien sin necesidad de configurar reglas especiales

e. Protect X

Deja algunos puertos abiertos y otros como cerrados. Toma nota desde donde te has conectado y el puerto. Facilita la información de registro IP.

f. Sygate Firewall

Interfaz futurista, viene configurado con un alto nivel de seguridad.

g. Win Route Pro

Es un servidor Proxy, filtra las direcciones de origen tanto como de destino, entrantes y salientes. No consume recursos del sistema y no es necesaria la instalación de un sw.

h. Zone Alarm

No solo detecta todos los accesos desde Internet si no que da control de los programas que intentan acceder a Internet. Puedes seleccionar los niveles de protección y bloquear el acceso a Internet tras un determinado tiempo.

i. At Guard

Permite definir reglas para todo, es rápido y se tiene control de lo que está sucediendo. Bloquea la publicidad no deseada, lleva un log de fecha, hora, URL, IP, bytes enviados y recibidos y tiempo de todas las conexiones Web.

j. Esafe Desktop

Consume muchos recursos del sistema, se puede prohibir el acceso total o parcial a tu ordenador.

k. Freedom

Es muy fácil de instalar, los puertos pasan a modo invisible y puedes navegar en Internet de manera anónima.

l. Hacktracer

Puede identificar al atacante, ya que cuenta con un programa que incorpora un mapamundi con la ruta del ordenador del atacante. Es fácil de instalar y por defecto todos los puertos pasan a modo invisible.

7.10. CONCLUSIONES

Mas allá del modelo utilizado, hay varias consideraciones finales a tener en cuenta para evitar las amenazas de una exposición a Internet permanente.

En primer lugar, es muy importante conectarse siempre a Internet con algún tipo de protección, como la que brindan los antivirus y los firewalls.

Como todos los temas relacionados con la seguridad informática, no hay soluciones definitivas que resuelvan todos los problemas. Es necesario monitorear con

frecuencia el comportamiento del sistema y mantenerlo actualizado para no llevarse sorpresas en el futuro.

Y lo más importante, un firewall por definición nos protege de los accesos no autorizados, ¿pero qué pasa con los accesos autorizados? La mayoría de las violaciones de seguridad modernas tienen que ver con mal uso de accesos autorizados, como los proporcionados por las páginas Web, servicios de correo, etc. Por ejemplo: un correo con un virus llega a su destinatario a través del firewall, que tiene una regla que permite pasar los mensajes de correo electrónico...

Mantenerse informado y una actitud proactiva son claves para evitar la falsa sensación de seguridad de la que son víctimas muchos usuarios, al pensar que con un firewall estarán protegidos de todos los males. Es necesario recordad que el firewall es la primera línea de defensa. No debería ser la única.

CAPITULO 8. IDS e IPS.

Es importante la utilización de IDS e IPS porque no importa que tan buena sea la seguridad establecida, siempre habrá alguien que pueda violarla, es por esta razón que existe esta tecnología para poder saber si alguien ha logrado penetrar las defensas establecidas y poder tomar medidas al respecto.

Forman parte integral de la estrategia de seguridad defensa en profundidad ya que con la implementación de estos se logra otro nivel de protección que apoya a los demás niveles defensivos establecidos.

Puntos clave.

- Conocer la importancia de estas tecnologías.
- Saber que se puede esperar de un IDS e IPS
- Tipos existentes de IDS e IPS
- Conocer las tecnologías utilizadas para la detección de intrusos
- Mostrar la forma de reacción de los IDS e IPS
- Conocer las diferencias entre IDS e IPS
- Dar algunas características y limitaciones
- Proveer de criterios generales de elección de IDS e IPS.

8.1 IDS: SISTEMAS DE DETECCION DE INTRUSOS (INTRUSION DETECTION SYSTEM).

La detección de intrusos monitoriza redes de computadoras y sistemas en busca de violaciones de políticas de seguridad. Los IDS están compuestos por 3 elementos funcionales básicos:

- Una fuente de información que proporciona eventos de sistema.
- Un motor de análisis que busca evidencias de intrusiones.
- Un mecanismo de respuesta que actúa según los resultados de motor de análisis.

Un Sistema de Detección de Intrusión (IDS) es un componente importante de una estrategia integral de seguridad de la empresa. Los productos IDS alertan en tiempo real a los administradores de seguridad de alguna actividad sospechosas que ocurren en sus sistemas y redes.

Los IDS ayudan a que se preparen y a que controlen los ataques. Esta meta se logra colectando información de una colección variada de sistemas y enlazando redes, luego analizando la información en busca de síntomas de problemas de seguridad. Los sistemas de detección de intrusión de siguiente generación le permiten al usuario especificar respuestas en tiempo real para las violaciones. Las tecnologías de valoración de vulnerabilidad, comprueban sistemas y redes en busca de problemas y errores de configuración que representan vulnerabilidades de seguridad. La detección de intrusión y las tecnologías de valoración de vulnerabilidad le permiten a las organizaciones protegerse de pérdidas asociadas con problemas de seguridad de la red.

8.1.1 Porque usar los IDS.

¿Cómo complementa la detección de intrusión a los firewalls?. Una forma de caracterizar la diferencia es clasificando la violación de seguridad por *la fuente:* si vienen de fuera de la red de la organización o desde el interior.

Los Firewalls actúan como una barrera entre redes corporativas (interno) y el mundo exterior (la Internet), y filtra tráfico entrante según unas normas de acción sobre seguridad.
Ésta es una función valiosa y sería suficiente protección de no ser por estos hechos:

- **No todo acceso a Internet pasa a través del firewall**. Los usuarios, por varias razones van de pasivos a la impaciencia, algunas veces colocan conexiones no autorizadas usando módem en sus sistemas conectados a la red interna y acceden hacia Internet. El firewall no puede mitigar el riesgo asociado con las conexiones que nunca ve.
- **No toda amenaza se origina fuera del firewall**. Una inmensa mayoría de pérdida debido a los incidentes de seguridad es atribuida a las personas al interior de la organización. Otra vez, el firewall sólo ve tráfico en las fronteras entre la red interna e Internet. Si el tráfico viaja a través de aberturas de seguridad y nunca fluye a lo largo del firewall, no puede ver los problemas. A medida que las organizaciones utilizan más fuertemente la encriptación para asegurar archivos y conexiones públicas de la red, el enfoque de los adversarios se hará en esos lugares en la red en la cual la información de interés no esta tan protegida: La red interna. Los sistemas de detección de intrusión son la única parte de la infraestructura que está al tanto del tráfico en la red interna. Por consiguiente, se pondrán aun más importantes como las infraestructuras de seguridad evolucione.

- **Los Firewalls están sujetos a agresiones y estrategias**. Los firewalls han sido ampliamente publicitados desde que los primeros firewalls fueron presentados.
  Una estrategia común de ataque es utilizar un túnel para sobre pasar a través de las protecciones del firewall. El túnel es la práctica de encapsular un

mensaje en un protocolo (eso podría ser bloqueado por filtros del firewall) dentro de un segundo mensaje.

8.1.2 Beneficios Reales

a. **Presentan un mayor grado de integridad.**

Los sistemas detectores de intrusos, ya que monitorean la operación de los firewalls, routers, servidores de manejo de claves y archivos críticos en otros mecanismos de seguridad, proveen capas de protección adicionales a un sistema seguro. La estrategia de un asaltante de sistemas a menudo será atacar o anular dispositivos de seguridad que protegen el blanco buscado. Los sistemas detectores de intrusos pueden reconocer estas primeras marcas de ataque, y potencialmente responden a ellos, disminuyendo el daño. Además, cuando estos dispositivos fallan, debido a la configuración, ataque, o error de usuario, los sistemas detectores de intrusos pueden reconocer el problema y puede notificar a las personas indicadas.

b. **Dan sentido a los sistemas de fuentes de información.**

Los seguimientos a los Sistemas Operativos y otros logs de sistema son un tesoro de información acerca de que sucede en los sistemas internos. A menudo estos son incomprensibles, aun para expertos administradores de sistema y oficiales de seguridad, los sistemas detectores de intrusos les permiten a los administradores organizar y comprender estas fuentes de información, a menudo revelando problemas antes de que ocurra algo fatal.

c. **Rastrean la actividad del usuario desde el punto de entrada al punto de salida o impacto.**

Los sistemas detectores de intrusos le ofrecen mejoras en las protecciones del perímetro como los firewalls. Los asaltantes expertos a menudo pueden penetrar en los firewalls; por consiguiente, la habilidad para relacionar la actividad correspondiente a cada usuario en particular es crítica para mejorar la seguridad.

d. **Reconocen y reportan alteraciones de archivos.**

Ya que colocar virus en los archivos de sistemas críticos es una técnica estándar de ataque, de modo semejante, la alteración de archivos críticos de información para camuflar la actividad ilegal, dañar reputaciones, o cometer fraude es común. Las herramientas de evaluación de integridad de archivos utilizan sumas de verificación para entregar estos archivos sin alteración, en el caso de un problema, rápidamente averiguan la extensión del daño. Pueden localizar errores en su configuración de sistema que tienen implicaciones de seguridad, algunas veces corrigiéndolas si el usuario lo desea.

e. **Reconoce cuando el sistema esta sujeto a un ataque en particular.**

Los productos de evaluación de vulnerabilidad también le permiten al usuario de sistema rápidamente determinar qué ataques deberían ser de preocupación para ese sistema, automáticamente registrando los resultados de los intentos de ataque, estos productos también proveen un chequeo valioso de nuevas instalaciones y configuraciones de infraestructura de seguridad.

Es difícil para un administrador de sistema determinar que su firewall esta configurado incorrectamente hasta que descubra que un asaltante ha penetrado exitosamente.

f. **Desahogan al equipo de administración del sistema de la tarea de monitorear el Internet en busca de los últimos ataques de intrusos.**

Muchas herramientas de detección de intrusión y de evaluación vienen con bases de datos extensivas con las firmas de ataque y se compara con el sistema que se quiere proteger. Las empresas desarrollando estos productos tienen a un personal experto que monitorean Internet y otras fuentes en busca de nuevas herramientas de ataque y técnicas. Luego usan esta información para desarrollar firmas nuevas que son provistas a los clientes para la descarga en sitios Web.

g. **Hacen posible la administración de la seguridad de los sistemas por personal poco experimentado.**

Unas herramientas de detección de intrusión y evaluación le ofrecen aquellos que no tienen experiencia en seguridad la habilidad de manejar características pertinentes a la seguridad de sus sistemas con una interfaz de fácil manejo.

Éstas son basadas en Windows, pantallas paso a paso para configurar las reglas de detección.

h. **Proveen líneas guías que asisten para establecer una política de seguridad.**

Muchos detectores de intrusos y productos de evaluación son parte de “suites” de seguridad que incluyen herramientas de construcción de política de seguridad. Estas proveen guías de fácil entendimiento para construir normas de actuación sobre seguridad.

8.1.2.1 Las expectativas poco realistas

a. **No son balas de plata**

La seguridad es un área complicada con dificultades y posibilidades innumerables. En redes, por ejemplo, Sólo se requiere de una vulnerabilidad en una máquina para permitirle a un adversario obtener acceso y potencialmente hacer estragos en toda la red. El tiempo que toma para que esto ocurra es minúsculo. No hay soluciones mágicas para los problemas de seguridad en redes, y los productos de detección de intrusión no son la excepción para esta regla. Sin embargo, como parte integral de de la seguridad pueden jugar un papel vital en la protección de sistemas.

b. **No pueden compensar la debilidad en los mecanismos de identificación y autenticación*.***

Aunque los lideres en la investigación de detección de intrusión afirman que el análisis estadístico sofisticado del comportamiento del usuario puede asistir en la identificación de una persona en particular solamente observando su actividad en el sistema, este hecho esta lejos de se demostrado. Por consiguiente, todavía debemos confiar en otra manera de identificar y autenticar usuarios. Esto es más conveniente apoyándose en fuertes mecanismos de autenticación. Una infraestructura de seguridad que incluye un buen mecanismo de identificación y autenticación, y un IDS es más fuerte que un sistema que tiene solo uno o el otro.

c. **No pueden manejar ataques de exploración sin intervención humana.**

En ambientes muy seguros, los incidentes ocurren. Para minimizar la ocurrencia de incidentes (y la posibilidad de que resulte en daño) se debe implementar *manejo de incidentes.* Se debe investigar los ataques, determinar, donde fue posible, la parte responsable, luego diagnosticar y corregir la vulnerabilidad que permitió que el problema ocurriera, reportando el ataque y detalles a autoridades donde se requiera. En algunos casos, especialmente en aquellos que involucran un atacante dedicado, encontrar el asaltante, luego seguir los cargos criminales en contra del asaltante es la única forma para hacer que los ataques cesen. Sin embargo, el sistema de detección de intrusión no es capaz de identificar a la persona en el otro extremo de la conexión sin intervención humana. Lo mejor que puede hacer es identificar la dirección IP del sistema que sirvió como punto de entrada del atacante, el resto depende de la persona encargada de manejar los incidentes.

d. **No pueden intuir las políticas de seguridad que satisfacen una empresa.**

   Los sistemas expertos de detección de intrusión aumentan en valor cuando se les permite funcionar como ambas, alarmas y motores de detección de ataques y manejo de políticas.

   Estas funciones no pueden solo ubicar al intruso que ataca un servidor de archivos, sino que también pueden ubicar al programador accediendo al sistema de planillas después de horas. Sin embargo, esta conformidad de política de inspección puede existir sólo si hay una política de seguridad que sirva de plantilla para construir firmas de detección.

e. **No pueden compensar las debilidades en los protocolos de red TCP/IP y muchos otros protocolos de red que no realizan fuerte autenticación de direcciones de origen y del destino.**

   Esto quiere decir que la dirección origen se refleja en los paquetes que portan un ataque que no necesariamente corresponde a la fuente *verdadera* del ataque. Es difícil de identificar quien es el atacante del sistema; Cuesta mucho probar la identidad de un asaltante en un tribunal de ley.

f. **No pueden compensar problemas en la calidad o integridad de la información que el sistema provee.**

Las fuentes de información de sistema son extraídas de una colección variada de puntos dentro del sistema. A pesar de los mejores esfuerzos por parte de los fabricantes de sistemas, muchas de estas fuentes son basadas en software; como tal, los datos están sujetos a alteración por parte de los asaltantes. Muchas herramientas de hacking como “cloak” y “zap” que buscan los “log” del sistema, para selectivamente borrar los registros correspondientes al tiempo del ataque y cubrir las huellas de los intrusos. Esto argumenta a favor del valor de la integración, algunas veces redundantes, fuentes de información; cada fuente adicional aumenta la posibilidad de obtener información no corrompida por un asaltante.

g. **No pueden analizar todo el tráfico en una red con mucha actividad.**

La detección basada en redes de intrusión es capaz de monitorear tráfico de una red, pero sólo para un punto. Primero, determinado el punto de ventaja de los detectores de intrusión basado en redes que se apoya en adaptadores de red para operar en modo promiscuo, en el cual no todos los paquetes son visibles para el sistema. Segundo, mientras los niveles de trafico se elevan los niveles de carga de procesamiento se vuelven elevadísimos y el motor de análisis falla. De hecho, los fabricante se caracterizan por el máximo ancho de banda en el cual demuestran sus productos para operar sin perdía con un análisis que cubre el 100% a 65Mbps.

h. **No siempre pueden ocuparse de problemas que involucran ataques a nivel de paquete.**

Hay debilidades en captura de paquetes basados en detectores de intrusión. El corazón de las vulnerabilidades involucra la diferencia entre la interpretación que el IDS le da al resultado de una transacción de red y el nodo destino para el manejo real de la transacción de esa sesión de red. Por consiguiente, un adversario experimentado puede enviar series de paquetes fragmentados o alterados que eluden la detección. Peor aún, un adversario puede usar esta clase de manipulación de paquetes para lograr un ataque de negación de servicio en el IDS mismo causado por desbordamiento de memoria ubicado en colas entrantes de paquetes.

i. **No pueden encargarse del hardware moderno de red y sus características.**

Tratar con paquetes fragmentados también puede ser problemático. Este problema tiene ramificaciones serias cuándo uno considera redes ATM de alta velocidad que usan fragmentación de paquete como una manera de optimizar el ancho de banda. Otros problemas asociados con avances en tecnología de red incluyen el efecto de las redes conmutadas en la captura de paquete basadas en IDS. Como el objetivo de las redes conmutadas es establecer un segmento de red por cada host, el rango de cobertura para un sistema de intrusión es reducido a un solo host. Este problema puede ser mitigado en aquellos switches que tiene monitoreo de puertos o extendiendo la capacidad; Sin embargo, estas características no son universales en el equipo actual.

8.1.3 Tipos de IDS.

Existen básicamente 2 tipos de sistemas de detección de intrusos:

- Sistemas de detección de intrusos de red (nIDS, por sus siglas en inglés)
- Sistemas de detección de intrusos basados en “host” (hIDS, por sus siglas en inglés)

a. **Sistemas de detección de intrusos de red (nIDS)**

Estos detectores actúan desde el exterior de los sistemas que protegen (en la red), identificando ataques hacia/desde los equipos que ellos vigilan en la red. Para la detección utilizan tablas de patrones de ataques, métodos estadísticos y métodos de inteligencia artificial para identificar agresiones potenciales hacia los sistemas de la organización, provenientes de otros equipos en la red o en Internet.

b. **Sistemas de detección de intrusos de host (hIDS)**

Actúan como un componente más de software dentro de los equipos que protegen; típicamente identifican alteraciones en aplicaciones y el sistema operativo, así como

eventos que pueden estar relacionados con un ataque, a través de diversas bitácoras del sistema operativo y de las mismas aplicaciones.

c. Sistemas de detección de intrusos distribuidos (DIDS)

En grandes organizaciones (multinacionales) o universidades (dónde hay diferentes facultades, departamentos, laboratorios...) un único sistema IDS no proporciona la flexibilidad necesaria para la heterogeneidad de los elementos de que se dispone.

Los sistemas **DIDS** (*Distributed Intrusion Detection System*) proporcionan este servicio de detección de intrusos para grandes redes.

La característica que los diferencia respecto a los sistemas NIDS tradiciones, es la presencia de dos elementos nuevos en su arquitectura:

- **Servidor central de análisis**: Es el centro del sistema DIDS y es el encargado de recibir toda la información procedente de los agentes y realizar un repositorio común de conocimiento. También realiza las funciones de control y sincronización de los diferentes nodos que forman parte del sistema.
- **Agente de red cooperativo**: Es un sistema autónomo encargado de la monitorización de una red, detecta posibles incidentes e informa al servidor central para que comunique a todos los nodos el ataque detectado así como las contra-medidas a realizar.

Dependiendo de la implementación, el agente puede llegar a tomar contra-medidas de forma autónoma (auque siempre informando y sometiéndose al servidor central).

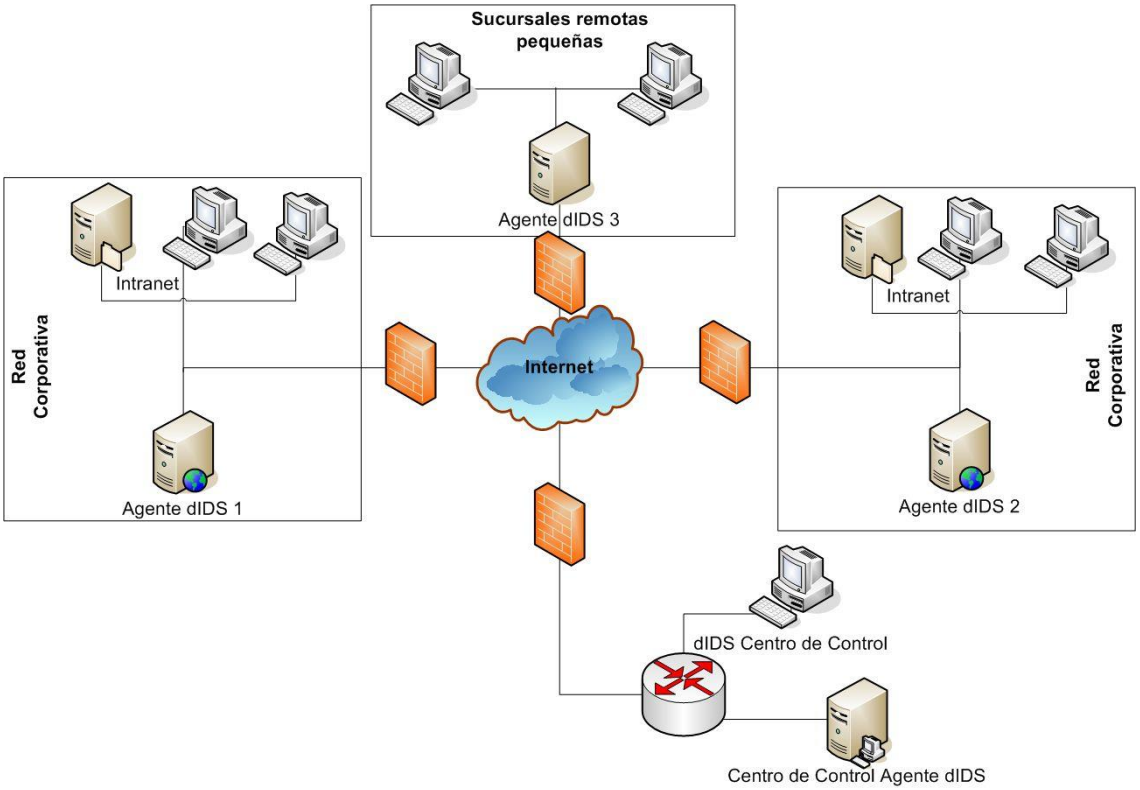


Figura 8.1. Ejemplo de sistema DIDS.

8.1.4 Ubicación de los nIDS.

Una vez explicados los componentes básicos de un sistema IDS, se ha de decidir de qué tipo han de ser los distintos sensores que utilizará el NIDS (*pull* o *push*), y finalmente se ha de concretar en que lugar o lugares de la red deben colocarse:

a. **Antes del firewall**:

   Esta arquitectura se basa en detectar todos los paquetes que llegan a nuestra red antes de ser filtradas por el firewall. De esta forma, realizamos una búsqueda de eventos de interés en todo el tráfico recibido sin interferencias de filtros del firewall.

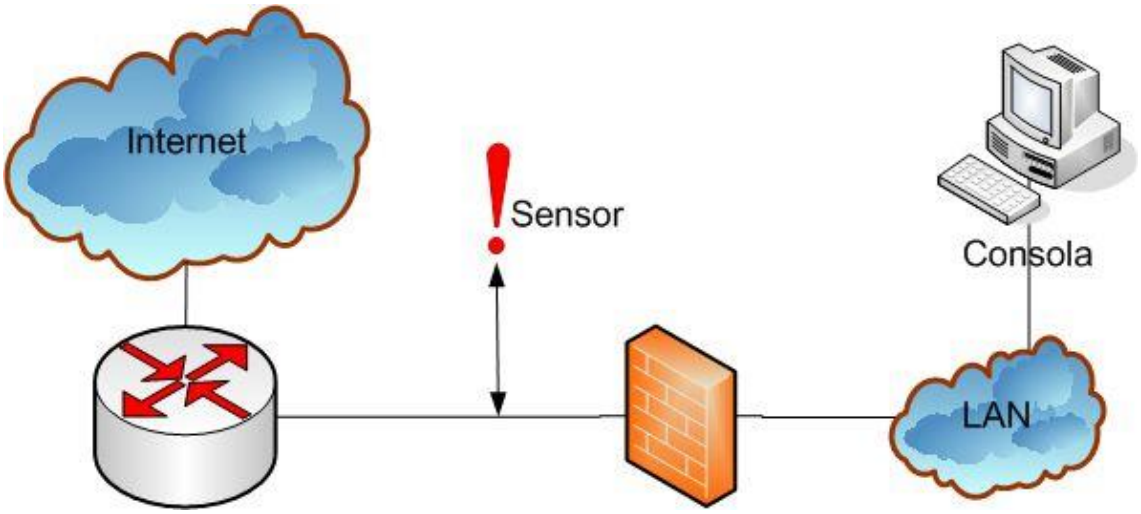


Figura 8.2. Sensores antes del firewall.

b. En el firewall o adyacente.

Consiste en situar el sensor en el propio firewall. De esta forma se evitan ataques de intrusos a los sensores externos y se eliminan muchas falsas alarmas, ya que se procesa únicamente el tráfico que el firewall deja pasar.

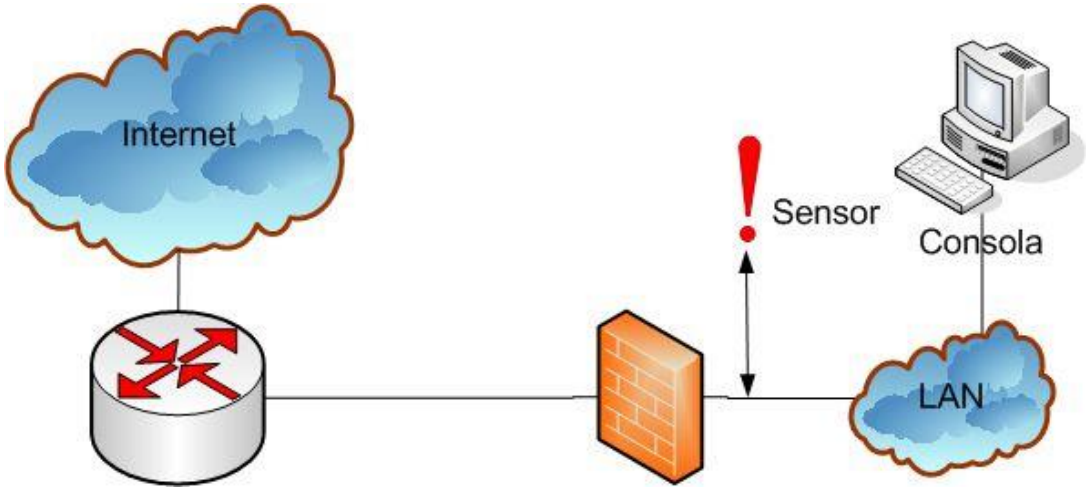


Figura 8.3. Sensores en el firewall.

c. Antes del firewall y en el firewall o adyacente.

Esta opción es más costosa pero ofrece mayor seguridad, ya que permite obtener lecturas del tráfico total y del tráfico filtrado por el firewall. Permite examinar la configuración del firewall y comprobar si filtra correctamente o no.

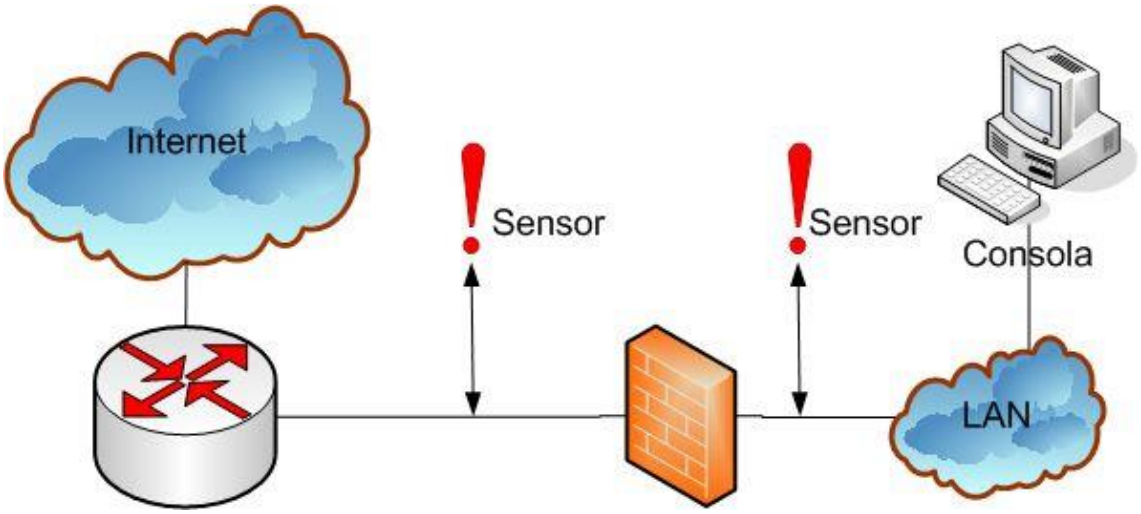


Figura 8.4. Sensores antes y en el firewall.

8.1.5 Arquitecturas de los nIDS.

Según la forma utilizada para el monitoreo del trafico de red, los NIDS se dividen en tres grupos distintos.

a. **NIDS basados en firmas**.
   Al igual que muchos antivirus, estos IDS se basan en la búsqueda de patrones conocidos (firmas) en el tráfico de la red.
b. **NIDS basados en anomalías**.
   Se basan en analizar el tráfico de la red creando estadísticas y asignándoles pesos. Cuando se detecta tráficos sospechoso, se confronta con las estadísticas anteriores y en función del peso asignado y la cantidad de ocurrencias del evento se dispara una alarma o no.
c. **Protocol modeling NIDS**.
   Estos sistemas de detección de intrusos buscan paquetes que contengan anomalías o configuraciones poco comunes de los protocolos de red (a fin de cuentas, los datos van encapsulados en distintos data gramas de distintos protocolos).

Los **sensores** (*sensors*) de un IDS son elementos pasivos que examinan todo el tráfico del segmento de red en búsqueda de eventos de interés.

Para evitar susceptibilidades, en caso de que el sensor no detecte eventos, incluirá una cadena de caracteres aleatoria para evitar enviar siempre el mismo paquete de cuando no existen eventos detectados.

La **consola** (*console*) de un sistema de detección de intrusos se encarga de recibir toda la información de los sensores y presentarla de forma entendible al operador. Desde la consola se pueden configurar los distintos sensores así como emprender acciones en respuesta a los datos recibidos de los sensores.

8.1.6 Tecnologías de detección en los IDS.

Existen diversas tecnologías utilizadas para la detección de intrusos; la tabla que se muestra a continuación resume las características de las tecnologías más utilizadas:

Tecnología especifica	**características**
Detección de patrones	Detectan ciertas actividades del sistema operativo o cadenas de bits en tráfico de red que indican actividad que pertenece o se relaciona con ataques conocidos.
Técnicas de inteligencia artificial	Identifican patrones de ataque o actividad anómala por medio de ciertos indicadores para un perfil (por ejemplo, a través de redes neuronales entrenadas para aceptar actividad cotidiana y disparar una alarma cuando hay una desviación considerable en los indicadores).

Métodos estadísticos	Identifican desviaciones numéricas en ciertos indicadores, basándose en perfiles previamente definidos de lo que constituye un ataque o actividad legítima.

Tabla 8.1. Tecnologías usadas en la detección de intrusos.

Como puede observarse, existen 2 enfoques en la aplicación de tecnologías de detección de Intrusos:

- Detectar aquello que es plenamente conocido (ataques o actividad legítima)
- Detectar aquello que es desconocido (actividad anómala, generalmente asociada con ataques)

Mientras que el primer enfoque da menos falsas alarmas, también está más limitado (no detecta ataques que no han sido definidos previamente), el segundo enfoque tiene una mayor capacidad de detección (ataques desconocidos por ejemplo), pero generan un número mucho mayor de falsas alarmas.

En cualquiera de los casos nunca es posible eliminar por completo el número de falsas alarmas dado que la capacidad de detectar un cierto número de ataques es proporcional en cierta medida al número de falsas alarmas que se detectan (entre más ataques se puedan detectar, mayor número de falsas alarmas)

8.1.7 Funcionamiento de los IDS.

Características principales de los sistemas de detección de intrusos.

La siguiente es una tabla comparativa de las diferentes características principales de los dos tipos de sistemas de detección de intrusos:

Característica	Basado en red (nIDS)	Basado en Host (hIDS)
Propósito	Protección simultánea de varios sistemas de cómputo; generalmente se protegen sistemas de cómputo críticos pero también se suelen utilizar para proteger sistemas de propósito general (gracias a su visibilidad).	Protección específica para sistemas de cómputo importantes, tales como servidores de producción y equipos de cómputo personales donde se almacena o procesa información crítica.
Visibilidad	Todo un segmento de red; pueden ver ataques dirigidos hacia equipos ubicados en el mismo segmento de red (si se utiliza un switch, el nIDS debe colocarse en un puerto de vigilancia para poder ver el tráfico de otros equipos). Si el switch o ruteador al que se conectan está en la frontera con Internet, entonces estos sistemas podrán ver los ataques desde Internet hacia toda la organización y viceversa.	Un único equipo; este sistema sólo puede identificar eventos en el equipo donde se encuentra instalado.
Nivel de operación	Diferentes capas de red	Eventos a nivel Sistema Operativo y aplicativo; en casos de sistemas híbridos pueden analizar tráfico de red, pero sólo aquel dirigido al equipo que protegen.
Recursos necesarios	Requiere de un equipo adicional a los sistemas que se protegen, con capacidad de procesamiento suficiente para revisar el tráfico de red del segmento que vigila.	Utiliza los mismos recursos del sistema que protege; por esta razón el sistema debe de contar con suficiente capacidad de procesamiento, almacenamiento y memoria para poder realizar sus actividades y las del sistema de

		detección de intrusos, sin que esto afecte su desempeño.

Tabla 8.2. Características principales de los hIDS e nIDS

Existen de igual manera requerimientos distintos en cada uno de estos sistemas de detección de intrusos. A continuación se muestran las dependencias de seguridad más importantes de los dos tipos de sistemas de detección de intrusos:

- **Sistemas de detección de intrusos de red (nIDS)**
  - Requiere emular el comportamiento de los sistemas que protege para mantener una sincronía entre su procesamiento y el de estos equipos; si existe sincronía, el sistema puede ser evadido (al ver por la red cosas distintas a las que ven los equipos que protege).
  - Requiere capacidad de procesamiento suficiente para evitar la pérdida de paquetes (con la consecuente asincronía que esto genera).
  - Requiere de visibilidad de los equipos que vigila (configurar puertos de vigilancia en switches para permitir a este tipo de sistemas vigilar el tráfico de los sistemas que protege puede tener consecuencias de desempeño en todo el segmento de red).

- **Sistemas de detección de intrusos de host (hIDS).**
  - Depende de la confiabilidad de bitácoras que analiza el hIDS y que son generadas por aplicaciones y sistemas operativos.
  - Requiere confianza en el sistema donde se va a instalar (un sistema de detección de intrusos de host no será muy útil en un sistema que ha sido comprometido anteriormente). Por esta razón se requiere fortalecer los sistemas donde se instalan este tipo de sistemas de detección de intrusos.
  - Impacta directamente al sistema que protege en caso de falla; dado que comparte los mismos recursos que el sistema y aplicaciones que

protege, puede generar problemas si el sistema de detección de intrusos falla.

- Es vulnerable ante un ataque directo (por residir dentro del mismo sistema).

Tanto los sistemas de detección de intrusos de red como los de host son controles de seguridad detectores, es decir, informarán en el momento de un incidente pero no tratarán de evitarlo (como un control preventivo); en algunos casos podrán corregir el problema (actuando como controles correctivos).

8.1.8 Respuestas para detección de uso indebido o ataques.

Algunos sistemas basados en NIDS le permiten especificar una reacción deseada para un problema detectado. Esta característica ha captado la atención de muchos administradores en el área de seguridad, especialmente con la frecuencia de ataques de *denial-of service (DoS)* la saturación de recursos de sistema han aumentado.

a. Alterar el Ambiente.

Una respuesta típica para un ataque detectado en la red es tomar medidas para alterar el ambiente del sistema bajo ataque. Esta alteración puede constar de terminar la conexión usada por el asaltante y reconfigurar los dispositivos de red para bloquear accesos futuros al sitio de la misma dirección origen. Los mecanismos de respuesta están dirigidos a permitirles a los administradores de sistema tomar un papel activo dentro de su autoridad para minimizar el daño asociado con un ataque detectado. Aunque es un tema popular de debate, contraatacar con atacar la fuente del ataque es mal aconsejado en este punto. TCP/IP, la base para las comunicaciones de Internet, le permite engañar cambiando la dirección IP origen; por consiguiente, el contragolpe en contra de la dirección origen podría dañar una parte inocente cuya dirección IP había sido utilizada para el ataque.

Otra característica valiosa de los sistemas de detección de intrusión es el cambio rápido en fuentes de información poniendo agentes y mecanismos de auditoria para colectar más información acerca de la conexión en cuestión. Esto también puede incluir colectar información que permite ataques de captura. Esta respuesta le permite al administrador de sistema colectar información que permite juicios más precisos acerca del intento del asaltante. También permite colectar información que podría ayudar en la ejecución de la ley u otras investigaciones para identificar a los responsables del ataque.

b. La validación

Los asaltantes experimentados a menudo tratarán de apuntarles a los sensores de detección de intrusión o el motor de análisis. En este caso, una respuesta de validación, en la cual los sensores y/o el motor de análisis son puestos en duda para determinar si continúan trabajando correctamente. Finalmente ***La notificación en Tiempo real***, la mayoría de los sistemas en tiempo real le permite a un administrador de sistema seleccionar una colección variada de mecanismos de alarma para hacerle saber de las partes responsables de los ataques detectados. Las alarmas pueden notificar a los empleados clave por email o mensajes de localizador emitidos instantáneamente con información acerca del problema. Un mensaje para la consola de sistema es estándar, y muchos sistemas permiten una colección variada de señales visuales y auditivas como parte de la alarma.

8.1.9 Limitaciones de los IDS.

Después de analizar los distintos tipos, arquitecturas y características de los sistemas de detección de intrusos, brevemente se explican que aspectos dejan más abiertos o no resueltos totalmente en la actualidad.

Los sistemas NIDS se basan en la observación del tráfico que circula por la red, esta única fuente de información le confiere una serie de limitaciones:

- Si alguien crea una puerta trasera ("*back-door*") o crea una red paralela en la intranet, probablemente los IDS no lo detectarán puesto que están pensados y configurados para el rango IP señalado.
- Si alguien se apropia de una cuenta y se autentica con el *login* y *password* correcto, tampoco será detectado.
- Si los sensores que alimentan al IDS o el propio IDS no funciona (la máquina, el sistema operativo o el programa no se encuentra operativo) no observaremos nada.
- Es importante realizar un seguimiento periódico de la actividad de estos programas, ya que el hecho de tenerlos instalados o hacer un simple *ping* a la máquina para ver si está operativa no es una política de seguridad aceptable.
- Muchas implementaciones de IDS soportan protocolos muy extendidos (usualmente basados en IP como FTP, HTTP...) pero no protocolos de usos minoritarios como el IPX/SPX o SNA. Existen muchos "*exploits*" disponibles para estos protocolos que pasarán inadvertidos en nuestra red. Si utilizamos Novell, NetBIOS, SNA... debemos tener en cuenta este punto.
- Los IDS tienen un máximo de capacidad de proceso, por lo que en momentos de mucho tráfico suelen descartar los paquetes que no pueden procesar.

  Raramente un IDS avisa de este punto, con lo que es conveniente calibrar periódicamente si nuestro IDS es capaz de soportar realmente toda la carga de la red (accesos a discos, swap, filtros muy complicados...). No hay que olvidar que usualmente un IDS no es más que un programa que funciona en una computadora.

Por otro lado, un IDS basado únicamente en la búsqueda de firmas (al igual que muchos antivirus) presenta dos grandes problemas:

b. El número de firmas va aumentando cada año (actualmente existen más de 100.000 para los antivirus) y tan sólo refleja los ataques que han sido ya identificados y analizados.

En los informes de ataques recibidos, siempre salen reflejados los mismos ataques que en el resto de Internet. Esto es debido a que los nuevos ataques aún no han sido detectados y documentados, con lo que no existe una firma a

la que asociar el ataque recibido, lo que puede crear una falsa sensación de seguridad al ver que detectamos siempre los mismos ataques.

b. En el caso de una red con cientos de computadoras, se pueden detectar ataques ya conocidos por el IDS.
Por otro lado el responsable de los ataques muy conocidos que detecta el IDS puede ser ignorado como un aprendiz de hacker (*script-kiddie*). ¿Quien nos garantiza que no irá "incrementando" probando otros ataques no documentados que no detectemos?

El uso de otras técnicas de seguridad que complementen a los sistemas de detección de intrusos (como basarse en la estrategia Defensa en profundidad) es vital para conseguir un sistema de seguridad fiable y eficaz.

8.1.10 Clasificación dependiendo del monitoreo.

a. Basado en aplicaciones.

Los sensores de IDS basados en aplicación colectan información a nivel de aplicación. Ejemplos de nivel de aplicación incluye "logs" generados por el software de administración de base de datos, servidores Web, o firewalls. Con la proliferación del comercio electrónico basado en Web, la seguridad progresivamente se enfocará en interacciones entre usuarios y programas de aplicación y datos.

Ventajas.

- Monitoreo a nivel de aplicación.
- Esta forma de operar permite apuntarle a actividades sospechosas en el sistema (por ejemplo se puede monitorear a un usuario utilizando una característica de una aplicación en particular).

Desventajas:

- Las vulnerabilidades del nivel de aplicación pueden debilitar la integridad del monitoreo y modo de detección basado en aplicación.

b. Basado en Hosts.

Los agentes de detección de intrusión basados en hosts (también llamados l*os sensores)* colectan información reflejando la actividad que ocurre en un sistema particular. Esta información está algunas veces en forma de auditoria de rastreo del sistema operativo. También puede incluir “logs” de sistema, otros “logs” generados por los procesos del sistema operativo, y contenidos de objetos de sistema que no se reflejan en los mecanismos de auditoria y “logs” de sistemas operativos estándar.

Ventajas:

- Los sistemas pueden monitorear acceso de información en términos de “quien accedió qué”.
- Los sistemas pueden trazar un mapa de actividades problemáticas a un específico ID de usuario.
- Los sistemas pueden rastrear cambios de comportamiento asociados con el uso indebido.
- Los sistemas pueden funcionar dentro ambientes encriptados.
- Los sistemas pueden funcionar dentro de ambientes de redes conmutadas.
- Los sistemas pueden distribuir la carga asociada con el monitoreo a través de hosts disponibles en redes grandes, por consiguiente reduciendo el costo de implementación.

Desventajas:

- La actividad de la red no es visible en detectores basados en hosts.
- Los mecanismos de auditoria pueden incurrir en recursos adicionales de implementación.
- Cuando el rastreo de auditoria es utilizado como fuente de dato, pueden tomar un almacenamiento significativo.
- Las vulnerabilidades del sistema operativo pueden debilitar la integridad de agentes basados en hosts y analizadores.

- Los agentes basados en hosts deben ser más específicos a la plataforma, la cual aumenta el costo de implementación.
- La administración y costos de implementación asociados con sistemas basados en hosts es usualmente mayor que en otros esquemas.

c. Basado en el Blanco.

El análisis de integridad permite implementar una estrategia de monitoreo enfocado y efectivo para los sistemas en los cuales la integridad de los datos e integridad de procesos es la prioridad. Este modelo monitorea archivos específicos, objetos de sistema y cambios en los atributos de los objetos de sistema, buscando en *el resultado* del proceso de ataque en vez de los *detalles* de los procesos de ataque. Algunos sistemas usan *sumas de verificación* para detectar violación de integridad.

Ventajas:

- Porque no depende de los registros históricos del comportamiento, el análisis de integridad pueden detectar las intrusiones que otras metodologías no detectarían.
- Este modelo permite detección confiable de ambos, la colocación y la presencia de ataques que modifican el sistema (Por ejemplo Caballos de Troya).
- Porque sus huellas e intrusiones son bajos, este modelo puede ser muy apropiado para monitoreo de los sistemas con comunicaciones o procesamiento modesto de ancho de banda.
- Este modelo es efectivo para determinar que archivo necesita ser reemplazado para recuperar el sistema, en vez de reinstalar todo desde la fuente original o el respaldo.

Desventajas:

- A merced del número de archivos, objetos de sistema y atributos de los objetos de sistema a los cuales se les calcula sumas de verificación, este modelo todavía podría demandar de una carga apreciable de procesamiento.
- El modelo no está recomendado para detección de procesos en tiempo real, como estos monitorean el resultado de ataques, no los ataques mismos mientras están en curso.

d. Basado en redes.

Los sensores de los detectores de intrusos basados en red colectan información de la red misma. Esta información es usualmente colectada por rastrear los paquetes, usando las interfaces de red puestas en el modo promiscuo; sin embargo, algunos agentes están integrados en los dispositivos de hardware.

Ventajas:

- Los datos vienen sin ningún requisito especial para revisar o poner mecanismos en bitácora. En la mayoría de los casos la colección de datos de la red ocurre con la configuración de una interfaz de la tarjeta de red.
- La inserción de un agente a nivel de red no afecta los recursos de datos existentes.
- Agentes a nivel de red pueden monitorear y pueden detectar ataques de red.

Desventajas:

- Aunque algunos sistemas basados en red pueden deducir del tráfico de red lo que esta pasando en los hosts, no pueden decir la salida de órdenes ejecutadas en el anfitrión. Éste es un problema en la detección, al distinguir entre error de usuario y fechoría.
- Los agentes basados en redes no pueden escanear protocolos o contenido si el tráfico de la red está encriptado.
- El monitoreo y detección de intrusos basado en red se pone más difícil en redes conmutadas modernas. Las redes conmutadas establecen un segmento

de red para cada host; Por consiguiente, los monitores basados en redes se reducen a monitorear a un solo host. Switches que soportan monitoreo o escaneo de puertos pueden al menos disminuir este problema.

- Los modelos de monitoreo basados en redes actuales no pueden manejar redes de alta velocidad.

e. Modelos integrados.

Algunos productos de detección de intrusión combinan sensores de aplicaciones y hosts basados en redes.

Ventajas:

- Agentes en aplicaciones, host, y niveles de red son usados, el sistema le puede apuntar a la actividad en cualquiera de todos los niveles.
- Es más fácil ver patrones de ataques sobre el tiempo y a través del espacio de la red; Esto es de valor en la recuperación de daño y de sistema; También auxilia en investigar el incidente.

Desventajas:

- No hay normas de industria con atención a la interoperabilidad de los componentes de los detectores de intrusos; Por eso es difícil o imposible integrar componentes de fabricantes diferentes.
- Los sistemas integrados son más difíciles de manejar e implementar.

8.1.11 Arquitectura de administración.

Los sistemas de detección de intrusos se pueden administrar de manera aislada o a través de arquitecturas de 2 y 3 capas:

Este diagrama ilustra un sistema de detección de intrusos de red (nIDS) que trabaja de manera aislada; los eventos se almacenan y reportan en el mismo sistema:

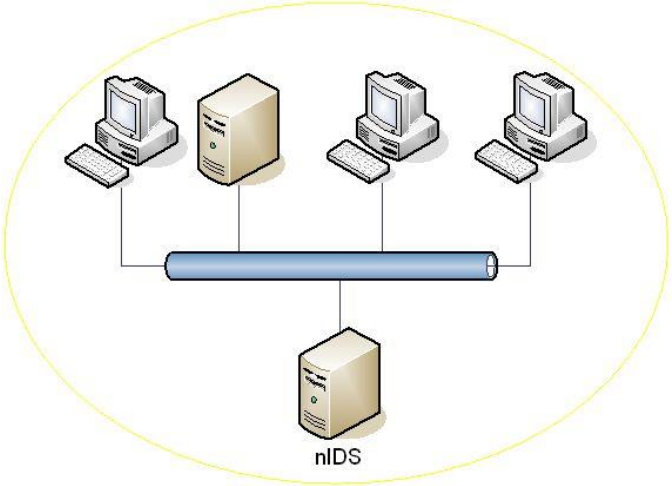


Figura 8.5. nIDS aislado.

En este siguiente diagrama se observar una arquitectura de 2 capas, donde los nIDS son sensores que se configuran y administran desde una consola central:

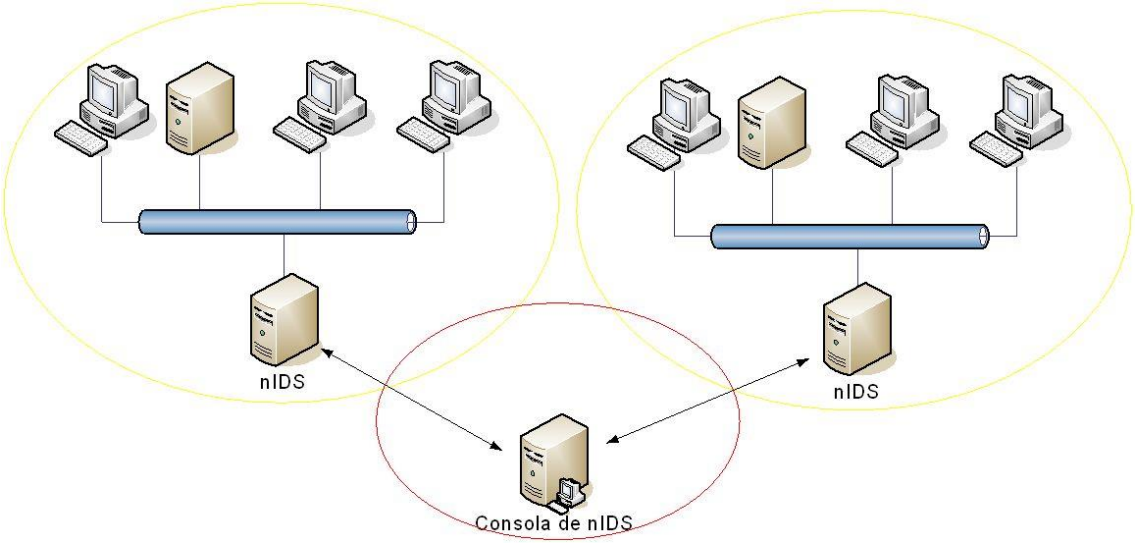


Figura 8.6. nIDS de dos capas.

El último diagrama ilustra una arquitectura de 3 capas para sistemas de detección de intrusos de red; el componente intermedio (administrador), concentra las bases de datos de los sensores que maneja. Además, procesa y aplica los cambios de configuración enviados desde la consola y envía a la consola reportes de actividad de los sensores:

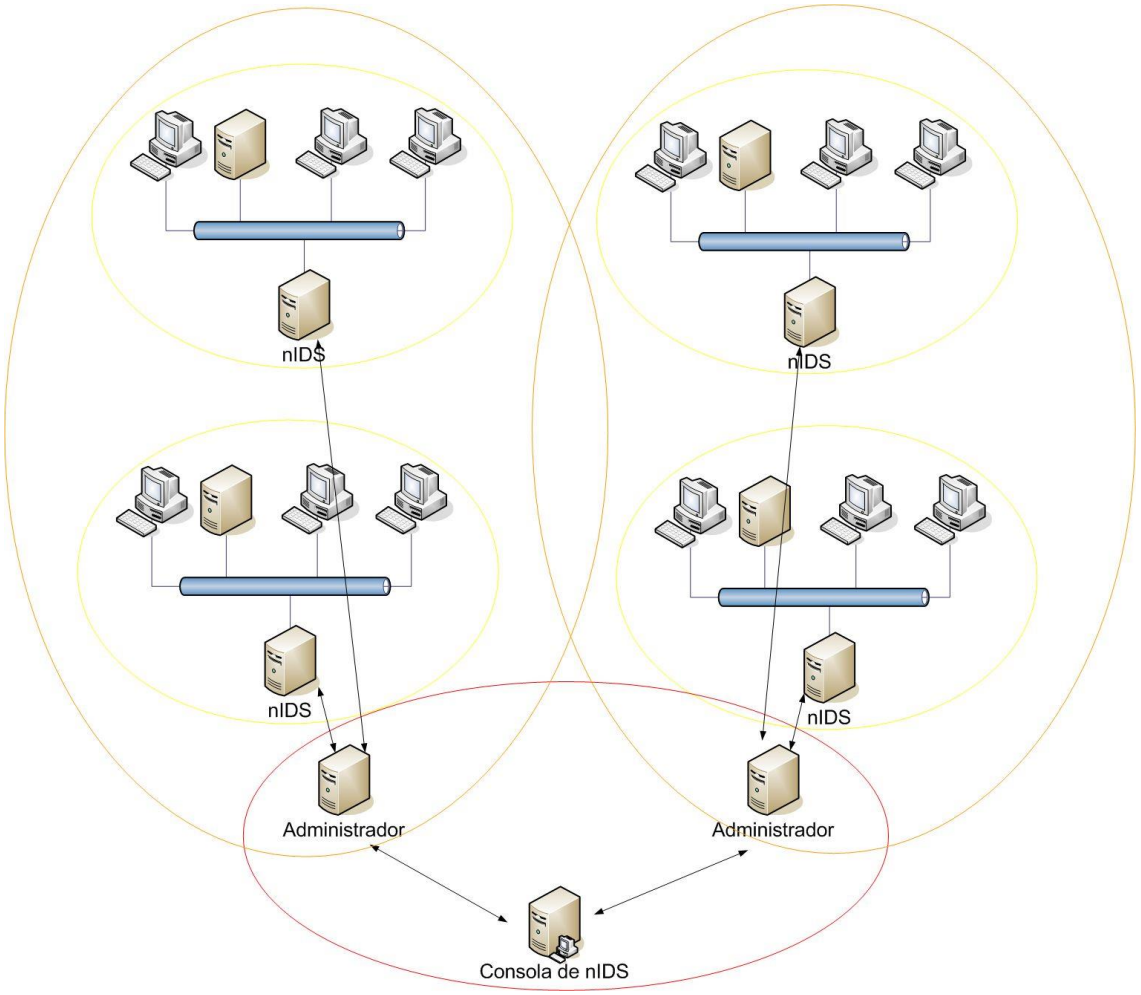


Figura 8.7. nIDS de tres capas.

En esta arquitectura de 3 capas es posible llevar a cabo cierto tipo de correlación en el sistema administrador, el cual concentra los datos de diversos agentes.

En el caso de sistemas de detección de intrusos basados en host (hIDS), las arquitecturas de administración son similares.

Arquitectura con un sistema de detección de intrusos de host (hIDS) que trabaja de manera aislada:

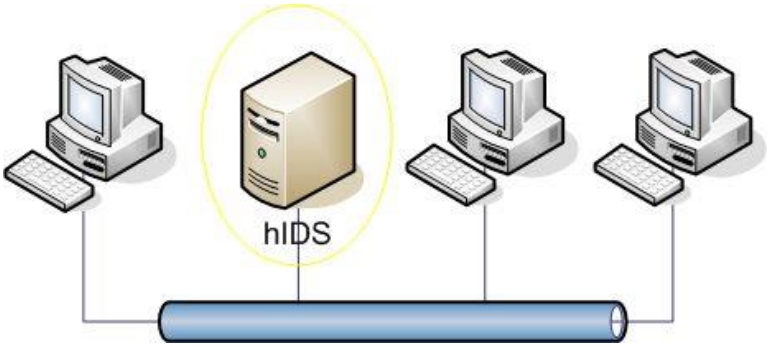


Figura 8.8. hIDS aislado.

a. Arquitectura de 2 capas (hIDS):

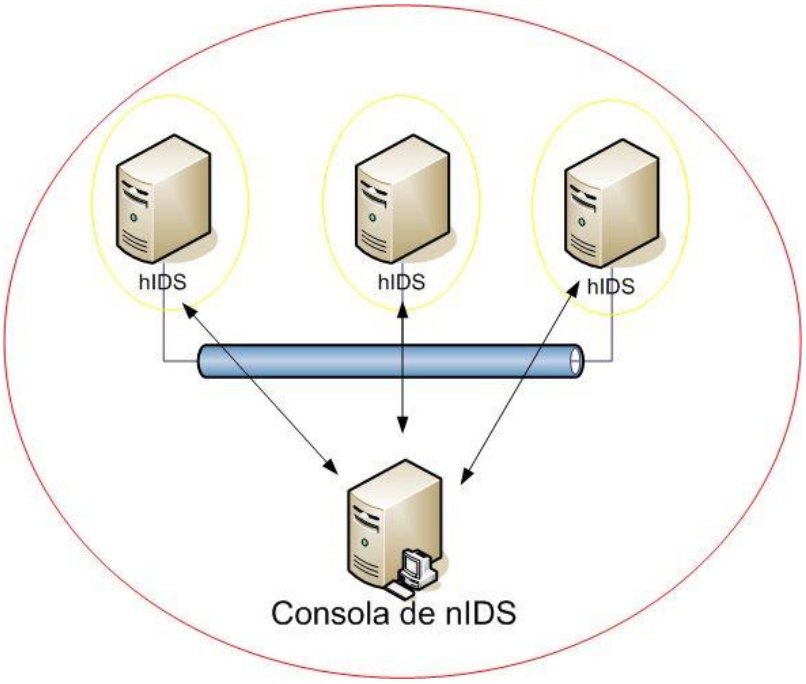


Figura 8.9.hnIDS de dos capas.

b. Arquitectura de 3 capas (hIDS):

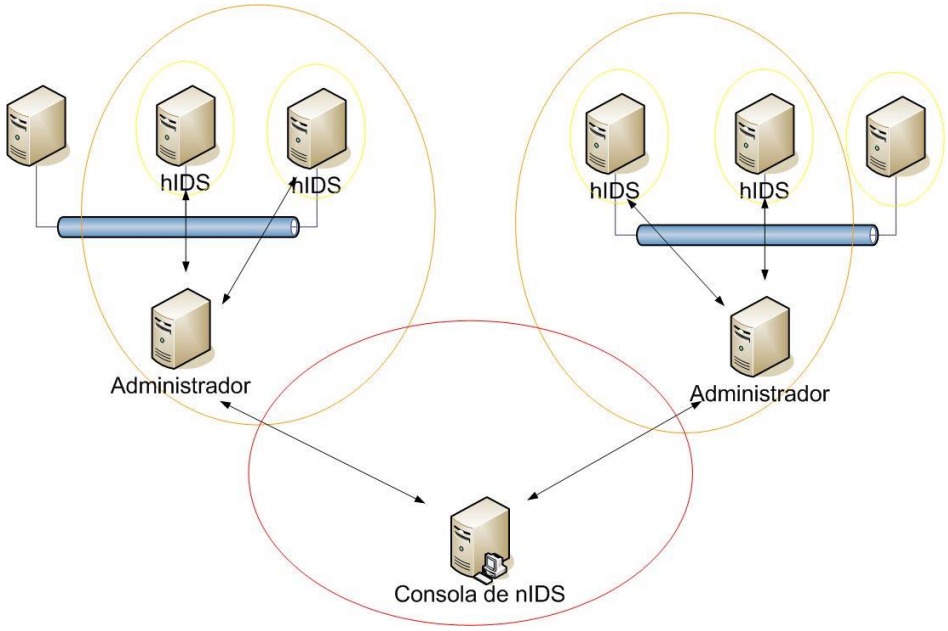


Figura 8.10.hnIDS de tres capas.

La selección de la arquitectura depende básicamente del tamaño de la organización, la cantidad de recursos que desea proteger, la importancia de estos recursos para la organización y los recursos que puede destinar para administrar la solución de sistema de detección de intrusos.

Es importante mencionar que ambos tipos de detectores de intrusos se complementan y se suelen implementar simultáneamente en organizaciones que requieren un alto nivel de seguridad. Algunos productos implementan una arquitectura híbrida para cumplir con este propósito; en estos casos, el agente híbrido se localiza dentro del equipo que protege con todas las características de un hIDS, pero incluye además la capacidad de revisar tráfico de red desde o hacia el equipo que vigila.

8.1.12 Arquitectura de operación.

Existen algunas opciones para la arquitectura de operación de un sistema de detección de intrusos.

En lo que se refiere a sistemas de detección de intrusos de red, existen básicamente 2 arquitecturas de operación: conexión en serie y conexión en paralelo.

a. Conexión en serie.

También conocida como arquitectura “inline nIDS”, se trata de un esquema de conexión donde el sistema de detección de intrusos etas siempre activo; el nIDS actúa como una especie de firewall, filtrando directamente aquél tráfico que considera relacionado con un ataque. Una falla en el nIDS, en este caso, tiene repercusiones sobre el desempeño y disponibilidad de la red. Es importante mencionar que no todos los sistemas de detección de intrusos de red tienen la capacidad de funcionar bajo este esquema; los sistemas de prevención de intrusos (IPS por sus siglas en inglés) que se mencionan más adelante, trabajan de manera similar a un IDS implementado con esta arquitectura.

El principal problema de esta arquitectura es que en caso de una falla en el nIDS, se pueden afectar seriamente las comunicaciones.

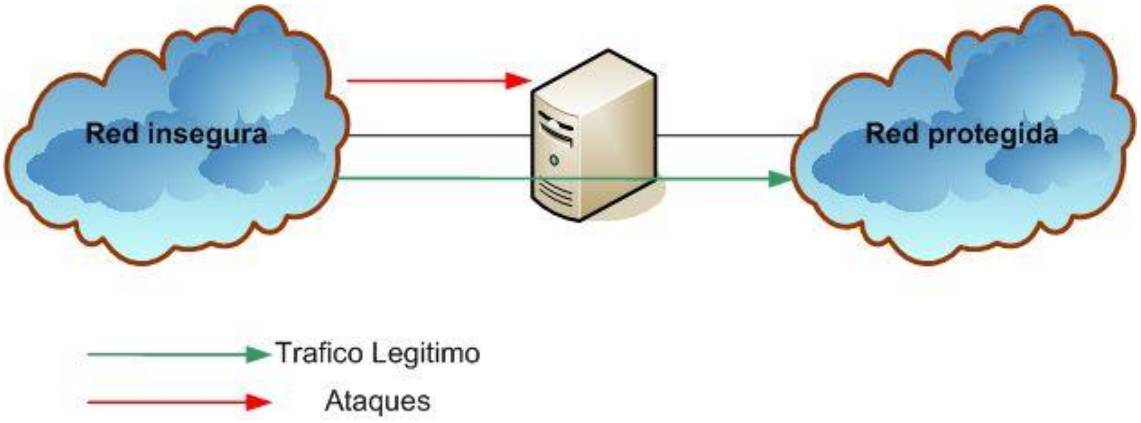


Figura 8.11. Conexión en serie de nIDS

b. Conexión en paralelo.

En esta arquitectura, el nIDS puede ser pasivo o activo (comunicándose con un firewall para que éste bloquee el origen de los ataques o enviando directamente

paquetes para cerrar la conexión, tanto al origen como al destino de la comunicación). En este caso el nIDS se ubica en lugar donde puede escuchar las comunicaciones pero no interviene directamente en la ruta del tráfico, por lo tanto, una falla en este tipo de sistemas no afecta el desempeño ni la disponibilidad de la red (tan sólo las funciones de seguridad que cubre). Es importante hacer notar que un ataque exitoso se puede llevar a cabo aún cuando esté siendo detectado por el nIDS en esta configuración; las opciones de cierre de conexión pueden reaccionar demasiado tarde.

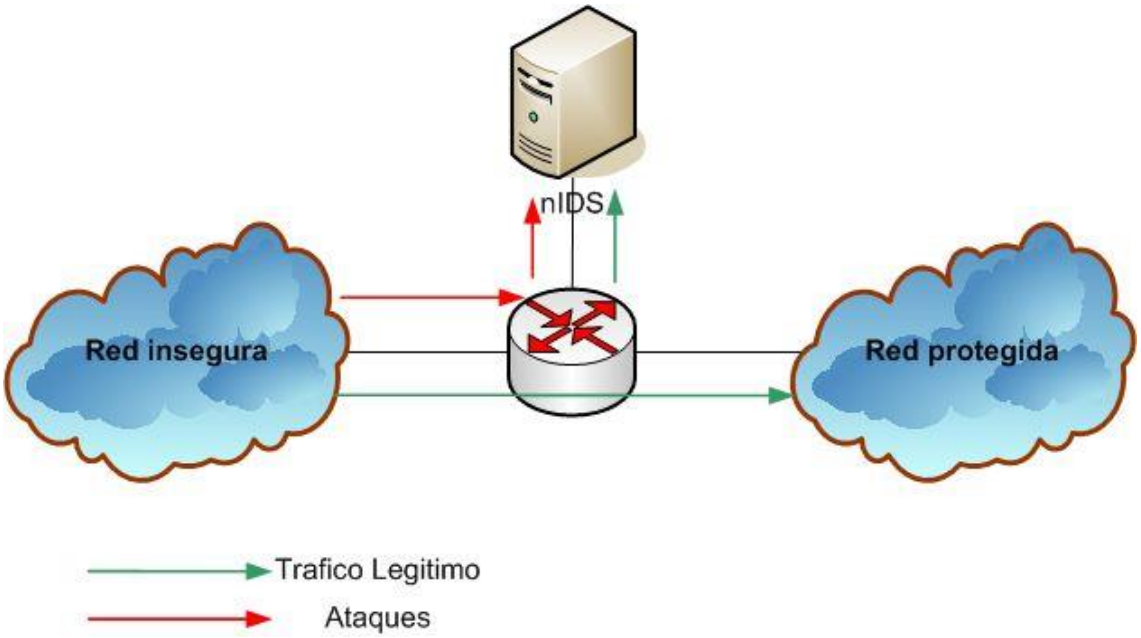


Figura 8.12. Conexión en paralelo nIDS.

Para la segunda opción (aunque se puede utilizar también con la arquitectura "inline"), se recomienda configurar una tarjeta de red adicional, dedicada únicamente a la administración (por un protocolo seguro) del IDS. La tarjeta de red que "escucha" ataques se configura en modo promiscuo y sin dirección de red para evitar que se envíe tráfico de red directo al nIDS; la 2ª tarjeta de red se conecta a un segmento distinto y suele configurarse un control de acceso restringido (firewall local y acceso con protocolo seguro a través de una red independiente para la administración).

Este esquema es recomendable ya que incrementa en gran medida la seguridad. En el caso de nIDS colocados en el perímetro de la red hacia Internet (delante del firewall), este esquema es necesario para evitar riesgos de seguridad. En este caso

particular el no separar el acceso de administración provocaría que el nIDS fuera accesible por la misma tarjeta de red por donde escucha, lo que lo convertiría en un blanco de ataques directos (dirección ip accesible desde la red).

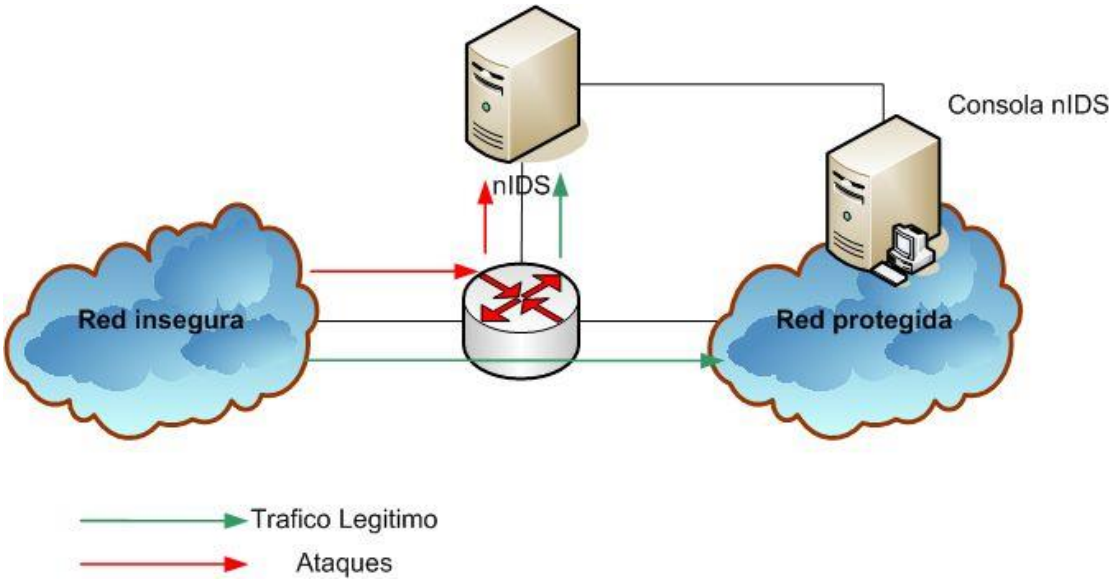


Figura 8.13. Conexión en paralelo nIDS mejorada.

La administración del nIDS a través de la misma tarjeta de red donde se detecta tráfico de ataque tiene los siguientes inconvenientes:

- Requiere de asignación de una IP ruteable (al menos desde un segmento de red interno); esto convierte al dispositivo en un recurso visible en la red y potencialmente puede ser objeto de ataques directos.
- Al usar la misma tarjeta de red para enviar y recibir datos, se puede se incrementa la carga de trabajo de este hardware y, en consecuencia, se puede afectar desempeño del sistema de detección de intrusos de red (por ejemplo, puede existir pérdida de paquetes).

En el caso de los sistemas de detección de intrusos de host (hIDS), existen pocas variantes en la arquitectura de operación, y éstas se enfocan principalmente en la reactividad del IDS. Un hIDS, al igual que un nIDS puede ser pasivo (sólo informa y registra los incidentes) o activo (trata de detener los ataques).

Tanto para sistemas de detección de intrusos de red como para sistemas de detección de intrusos de host, es necesario tener sumo cuidado cuando se configuran como controles activos, ya que es común que generen negaciones de servicio. El problema de la reactividad radica en el hecho de que los ambientes donde operan actualmente (red y sistema operativo) no tienen la capacidad de verificar integridad y autenticidad del origen de los eventos; esto se traduce en que todo puede ser falsificado.

Si el IDS no tiene todo el conocimiento necesario del ambiente, puede generar una negación de servicio en el momento inapropiado. Por ejemplo, un atacante puede enviar tráfico de ataque a través de un nIDS falsificando la dirección de origen, de manera que pareciera que proviene de un socio de negocio de la organización. Si el nIDS es configurado como activo, y no posee el conocimiento suficiente para poder identificar que se trata de la dirección de un socio de negocio, simplemente bloqueará este tráfico y pudiera, a la vez, bloquear otro tráfico legítimo de este socio de negocio.

La generación de falsas alarmas es un problema inherente de los IDS; a mayor capacidad de detección hay un mayor número de falsas alarmas.

8.2. ELECCIÓN DE UN IDS ESPECÍFICO.

Selección del tipo, cantidad y arquitectura de sistemas de detección de intrusos
La selección de la solución de detección de intrusos debe considerar diversos factores; estos factores se resumen en criterios de selección que se muestran a continuación:

CRITERIOS	**Sistemas de detección de intrusos de red (nIDS)**	**Sistemas de detección de intrusos de host (hIDS)**
Ubicaciones donde se recomienda instalar los sistemas de protección.	Segmentos de red con sistemas críticos que ofrecen servicios a través de la red.	Sistemas críticos de producción o que almacenan información confidencial.

	Subredes internas críticas. Servidores de una Zona desmilitarizada como por ejemplo: Servidores de Web, Correo electrónico, DNS, FTP y Acceso remoto. Subredes donde se conecta personal que maneja información altamente confidencial y subredes destinadas a la conexión de proveedores y personal externo.	Sistemas portátiles críticos Servidores ERP, servidores de Bases de datos corporativas, sistemas de seguridad (firewalls, antivirus, control de acceso, etc.). Equipos portátiles de personal que maneja información crítica de la organización (directores, gerentes, etc.)
Cantidad	Al menos uno por subred crítica. La cantidad de consolas y sistemas de administración depende de la arquitectura y producto seleccionado. El volumen de tráfico de red y filtros implementados entre segmentos de red pueden provocar que se requieran más de un sensor por subred.	Un sensor por cada sistema crítico. La cantidad de consolas y sistemas de administración depende de la arquitectura y producto seleccionado. En caso de sistemas conectados en “cluster” se puede considerar un sensor por equipo, para contar con una protección individual a nivel de sistema operativo.
Arquitectura recomendada	Sensores individuales si los puntos de control son pocos (3 o menos) 2 capas si existen varias subredes vigiladas 3 capas si existen varias redes independientes (oficinas en diferentes ciudades por ejemplo)	Sensores individuales si los equipos a vigilar son pocos (5 o menos) 2 capas si existen equipos ubicados en varias subredes vigiladas 3 capas si los equipos a ser vigilados se ubican en diferentes redes independientes (oficinas en diferentes ciudades por ejemplo)

8.3. IPS: SISTEMAS DE PREVENCIÓN DE INTRUSOS (INTRUSION PREVENTION SYSTEMS).

Los IPS son dispositivos de hardware o software encargados de revisar el tráfico de red con el propósito de detectar y responder a posibles ataques o intrusiones. La respuesta usualmente consiste en descartar los paquetes involucrados en el ataque o modificarlos (*scrubbing*) de tal manera que se anule su propósito. Es claro que este comportamiento los clasifica como dispositivos proactivos debido a su reacción automática a situaciones anómalas.

De alguna manera el comportamiento de los IPS semeja el comportamiento de los firewall ya que ambos toman decisiones con respecto a la aceptación de un paquete en un sistema. Sin embargo, la diferencia radica en el hecho que los *firewall* basan sus decisiones en los encabezados del paquete entrante, en particular los de las capas de red y de transporte, mientras que los IPS basan sus decisiones tanto en los encabezados como en el contenido de datos (*payload*) del paquete.

8.3.1. Los IPS como evolución de los IDS.

Para varios autores los sistemas de prevención de intrusos son la evolución de los sistemas de detección de intrusos, particularmente, se clama que los primeros ofrecen un manejo más efectivo de las intrusiones al tiempo que superan las dificultades inherentes de los IDS, en particular, la permisividad de los IDS ante las intrusiones.

El IDS se limita a detectar y notificar la intrusión a la persona encargada de recibir y responder las alertas (por ejemplo: el administrador de la red o el operador del IDS) quien debe tomar la acción correctiva pertinente, lo que es análogo a darse cuenta de un robo en un banco y limitarse a notificarle a la policía.
Por su parte, una vez el IPS detecta la intrusión la detiene de algún modo. En el caso de la analogía del robo, el IPS representa un guardia armado que reacciona de forma instintiva al ataque.

Vale la pena mencionar que el nivel de alertas de un IPS es considerablemente menor que el nivel de alertas producido por un IDS, puesto que el IPS se encarga de manejar la situación y sólo genera alertas si se le configura explícitamente para tal fin o en caso que la criticidad de los eventos y circunstancias lo amerite.

Es importante tener en cuenta que entre los IDS y los IPS hay una categoría especial de IDS que se denominan *IDS con respuesta activa*, que cumplen la función de detener las intrusiones descartando los paquetes relacionados con el ataque.

La diferencia principal entre los IDS con respuesta activa y los IPS es que estos últimos están en capacidad de inutilizar los paquetes involucrados en el ataque modificando su contenido, pero tal distinción parece no estar muy difundida y la mayoría de la bibliografía cataloga los IDS con respuesta activa como un tipo particular de IPS.

La propiedad inherente a los IPS de reaccionar automáticamente a las intrusiones (o lo que ellos determinan como tales) ciertamente disminuye significativamente el tiempo de reacción al ataque, pero también puede desencadenar eventos inesperados e inconvenientes cuando se reacciona ante un falso positivo (FP). Lo anterior indica que es indispensable la disminución de este tipo de caracterizaciones para que el IPS sea más preciso.

Las consecuencias de la intervención inoportuna e inesperada del IPS en caso de un falso positivo pueden ir desde la negación del servicio a los clientes hasta el aislamiento total de la máquina. Se comenta el caso de un IPS que erróneamente determinó que el servidor DNS de la empresa estaba haciendo un scan de puertos de la red y tomó la decisión de bloquear todo acceso a éste, produciendo un colapso en los aplicativos de red en la organización.

Por otro lado, las arquitecturas actuales para los IPS centralizan su funcionamiento en un solo punto lo que facilita su operación y administración, sin embargo, la

centralización disminuye la escalabilidad del sistema y convierte al IPS en un punto crítico, cuyo mal funcionamiento impacta negativamente a nivel de uso y de desempeño en la red sobre la que opera.

Finalmente, es importante notar que los IPS no son la “bala de plata” que hace desaparecer los problemas de seguridad, ni soluciona las falencias de los IDS, por ejemplo, los IPS no están en capacidad de detectar y mucho menos detener intrusiones sobre comunicaciones cifradas o detener intrusiones que ni siquiera son capaces de detectar.

De lo anterior se deduce que los IPS son un elemento en la arquitectura de seguridad y no se les puede considerar como una arquitectura *individual*. Es por esto que se recomienda adoptar un esquema de seguridad por capas o una estrategia de “*Defensa en profundidad*”.

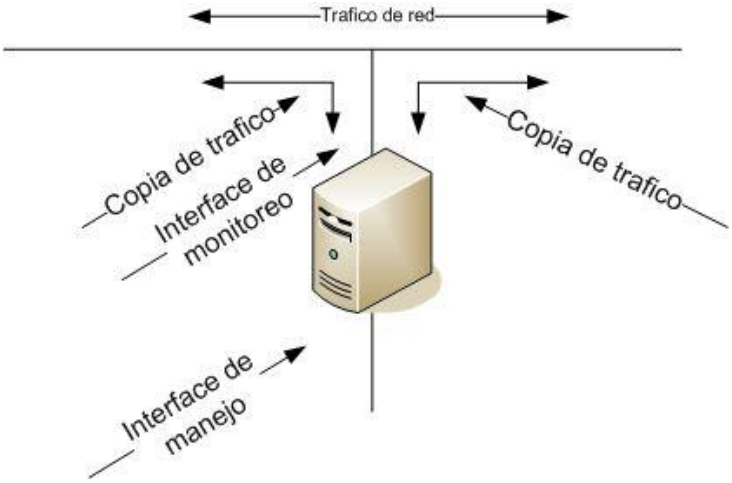
8.3.2. La evolución y las categorías de los IPS.

Es posible distinguir dos generaciones históricas de los IPS: los primeros, al detectar un ataque proveniente de una dirección IP determinada, descartaban todos los paquetes provenientes de dicha dirección -estuvieran o no relacionados con el ataque- (IPS de primera generación).

Posteriormente se refinó la anterior estrategia de tal manera que el IPS descartara únicamente los paquetes relacionados con el ataque identificado, permitiendo el tráfico de otros paquetes provenientes de la IP del atacante siempre y cuando no estuvieran relacionados con el ataque (IPS de segunda generación).

Por otro lado, es posible distinguir cinco categorías de IPS dependiendo de su funcionamiento, sus capacidades y su ubicación en la arquitectura de la red, tales categorías se describen a continuación:

a. Los IPS inline.



Este tipo de IPS usualmente se despliega en algún punto de la red como un *bridge* de nivel dos de tal manera que media entre los sistemas que protege y el resto de la red.

En adición a la funcionalidad típica de un *bridge*, el IPS inline revisa todos los paquetes en busca de la firma que define alguno de los ataques que está configurado para identificar. En caso que el paquete este “limpio”, el IPS le permite el paso (como un *bridge* normal), en caso contrario lo descarta registrándolo en un log. El IPS inline puede incluso permitir el paso de un paquete sospechoso modificando su contenido, de tal manera que el propósito del ataque se frustre sin que el atacante sepa que sus paquetes están siendo modificados.

Existen implementaciones de los IPS *inline* más elaboradas que pueden llegar a realizar consultas DNS reversas y *traceroutes* sobre la identidad del atacante, consignando los resultados obtenidos en un log de tal manera que se obtenga automáticamente información adicional sobre el autor del ataque.
Es importante tener en cuenta que los IPS inline son una evolución de los NIDS, en particular, de los NIDS basados en reglas (firmas). Debido a lo anterior, los IPS inline heredan las mismas limitaciones de éstos.

b. Switches de nivel de Aplicación.

Últimamente ha aumentado la tendencia a utilizar switches en la capa de aplicación, que funcionan de forma independiente a otros dispositivos de red y en su propio hardware optimizado para manejar grandes volúmenes de tráfico (entre uno y varios *Gigabits*).

La tarea principal de los *switches* de nivel siete (también conocidos como *switches* de contenido) es balancear las cargas de las aplicaciones distribuidas entre varios servidores, tomando decisiones de enrutamiento o conmutación a partir del *payload* de información de nivel.

El *modus operandi* recién descrito se adapta de forma precisa a lo que se espera del IPS, ya que revisa el contenido de datos del paquete y es posible configurarlo para que lo analice y descarte de forma eficiente en caso que su contenido concuerde con alguna firma preestablecida en el IPS.

Debido a lo anterior los switches de aplicación son los más efectivos (aunque usualmente costosos) a la hora de prevenir intrusiones, particularmente de negación del servicio.

c. Firewalls de aplicación/IDS.

A diferencia de los enfoques precedentes, los firewall de aplicación/IDS no funcionan al nivel de paquete. Éstos se instalan en cada host que se desea proteger adaptándose íntimamente con las aplicaciones que corren en el host que protegen. Para lograr lo anterior es necesario que antes de comenzar la fase de protección se ejecuten en modalidad de entrenamiento.

La modalidad de entrenamiento consiste en el proceso de identificación de patrones de comportamiento normales en el *host*. En particular se crea un perfil de relaciones frecuentes entre las aplicaciones y varios componentes del sistema como: el sistema operativo, otras aplicaciones, la memoria y los usuarios.

Una vez se han establecido los patrones de comportamiento normal, el IPS se comporta de forma similar a los IDS basados en detección de anomalías a la hora de

detectar las intrusiones.

Lo anterior hace de esta categoría de IPS los más efectivos a la hora de detectar y prevenir vulnerabilidades generadas por errores en la programación de las aplicaciones, además, debido a que se apoyan en la detección de comportamientos anómalos y no en la coincidencia de firmas, es posible prevenir intrusiones muy recientes para las cuales todavía no existe la definición de sus firmas específicas.

Por su parte, la desventaja principal de este tipo de IPS, al igual que los IDS basados en detección de anomalías, es que la fase de entrenamiento debe comprender absolutamente todos los comportamientos válidos, a fin que ningún comportamiento normal no aprendido se catalogue como anormal. Lo anterior puede traer graves.

d. Switches híbridos.

Los Switches híbridos son una combinación entre los firewall de aplicación/IDS y los Switches de nivel de aplicación. Al igual qué estos últimos, funcionan sobre dispositivos de hardware dedicados y optimizados para la inspección y manejo de paquetes, pero a diferencia de éstos se basan en políticas de aceptación de tráfico (comportamiento) válido de manera similar a los firewall de aplicación/IDS,

La fortaleza de esta aproximación radica en el conocimiento detallado del tráfico que debe aceptar y por consiguiente el que debe rechazar una aplicación o un host determinado.

e. Aplicaciones engañosas (deceptive).

Al igual que los *firewall* de aplicación/IDS, las aplicaciones engañosas aprenden el comportamiento de los servicios ofrecidos por cada uno de los host que protege. Una vez se detecta algún tipo de comportamiento sospechoso sobre un servicio/host existente o no, el IPS suplanta al servicio en caso que exista o lo simula en caso contrario, respondiendo al atacante y marcándolo de tal forma que sea posible

identificarlo y bloquearlo posteriormente.

8.4. CONCLUSIONES.

Se ha visto que la diferencia a nivel teórico entre los IDS y los IPS radica en la forma como reaccionan ante las intrusiones: los primeros se limitan a detectar y notificar de la intrusión mientras que los segundos toman acciones de algún tipo frente a tales eventos.

Debido a la anterior aseveración, se tiene que el uso de los IDS implica un corto lapso de tiempo para enterarse, analizar y determinar la acción correctiva a adoptar frente a la intrusión, para finalmente reaccionar manualmente al ataque.

Por esta razón, el fuerte de los IDS radica en su utilidad *a posteriori*, ya que ayudan a la reconstrucción del ataque para su posterior análisis.

Sin embargo, muchas veces es deseable detener el ataque de manera oportuna, campo en el cual los IPS son la solución adecuada, siempre y cuando estén debidamente configurados y puestos a punto con el fin de maximizar su nivel de precisión.

CAPITULO 9. CRIPTOGRAFÍA, ENCRIPTACIÓN Y AUTENTICACIÓN

Las funciones criptográficas son el pilar fundamental en la implementación de una VPN ya que proveen la seguridad necesaria para poder enviar los datos a través de un canal o medio de transmisión inseguro (Internet), mediante el uso de funciones que poseen un alto grado de seguridad y confiabilidad ya sea para la encriptación como para la autenticación de los datos.

En el presente capítulo se estudian los conceptos básicos acerca de la criptografía, encriptación y autenticación, además que funciones y algoritmos se utilizan para el diseño e implementación de una VPN mediante la utilización del protocolo IPSec. Así también, como estos contribuyen al fortalecimiento de la seguridad de redes, lo cual es logrado mediante el aseguramiento confiable de los datos que viajan a través del túnel VPN, poniendo en evidencia la contribución e importancia de estos dentro de la estrategia de seguridad “Seguridad en profundidad”.

Puntos clave

- Mencionar los conceptos básicos acerca de criptografía, encriptación y autenticación.
- Dar a conocer la importancia de la criptografía dentro de una red
- Describir los algoritmos de criptografía y encriptación disponibles que pueden ser utilizados con el protocolo IPSec.
- Detallar el uso de las llaves simétricas y asimétricas.
- Proveer información básica acerca de los algoritmos simétricos y asimétricos necesarios en la implementación del protocolo IPSec.
- Describir los métodos básicos para asegurar una VPN

9.1 INTRODUCCIÓN A LA CRIPTOGRAFÍA

El propósito de este capitulo es introducir la terminología y dar un breve vistazo de los conceptos de criptografía que relacionan a IPSec como un fundamento de las redes privadas virtuales. El pivote de cualquier tecnología VPN es su conjunto de funciones criptográficas. Cualquier persona no debería planear e implementar una VPN sin conocer que nivel de seguridad puede ser alcanzado con la tecnología incorporada en un producto específico. Después de todo, no se quiere ver la información importante como algo alcanzable cuando ésta viaja a través de canales inseguros.

9.2 TERMINOLOGÍA

Ahora se van a definir algunos conceptos básicos:

Criptografía: la criptografía es la ciencia de mantener los datos y las comunicaciones seguras. Para lograr este objetivo se utilizan técnicas como la encriptación, desencriptación y autenticación.

Cada procedimiento consiste en la transformación de datos utilizando métodos que son difíciles de revertir y pueden ser considerados como criptografía. El factor clave para fortalecer la criptografía es la dificultad de revertir los datos. Cualquier persona quedaría asombrado al conocer que mediante el uso de métodos simples para descifrar claves cualquier documento de un procesador de palabras ó un documento compreso le puede tomar minutos a un hacker el descifrarlos con una computadora normal.

La criptografía fuerte significa que un esfuerzo en cálculos computacionales es necesario para recuperar los mensajes originales sin conocer el propio procedimiento que hace la recuperación del mensaje irrealizable. En este contexto, irrealizable significa algo como esto: si todas las computadoras en el mundo estuvieran asignadas al problema, ellas tendrían que trabajar miles de años hasta que la

solución fuera encontrada. El proceso de recuperación es llamado criptoanálisis. Un intento de realizar un criptoanálisis es considerado un ataque.

Los algoritmos discutidos en el presente capitulo serán clasificados en tres categorías básicas:

- El primero usa el proceso de transformación de un solo camino (one-way) para alterar el texto normal en texto cifrado. Estos programas de transformación son típicamente referidos como algoritmos hash.
- El segundo usa el sistema de encriptación de llaves privadas (private key): llaves privadas asociadas
- El tercero usa el sistema de encriptación de llaves públicas (public key): llaves públicas asociadas

Existen otros nombres comunes para estos procesos de encriptación incluyendo los algoritmos simétricos (symmetric) y asimétricos (asymmetric) ó algoritmos de una llave(one-key) ó dos llaves (two-keys). Los algoritmos hash son también referidos como operaciones de encriptación sin llave (no-key) ó de llave cero (zero-key) porque como el nombre lo sugiere los algoritmos hash no utilizan llaves.

9.3 ENCRIPTACIÓN Y DESENCRIPTACIÓN – ALGORITMOS CRIPTOGRÁFICOS

La encriptación es la transformación de un mensaje original en una forma irreconocible con el propósito de ocultar su significado. La transformación opuesta, la que recupera el mensaje original es llamada desencriptación. La función matemática usada para la encriptación y desencriptación es el algoritmo criptográfico o cifrador (cypher).

La seguridad de un cifrador podría estar basada enteramente en mantener como este trabaja secretamente, en tal caso en un cifrador restringido. Hay muchos

inconvenientes para cifradores restringidos. Es muy difícil mantener en secreto un algoritmo utilizado por muchas personas. Si este es incorporado en un producto comercial, entonces es solo cuestión de tiempo y dinero el lograr revertirlo. Por estas razones, los algoritmos utilizados actualmente están codificados, por lo cual, la encriptación y desencriptación hacen uso de un parámetro importante, la llave secreta (key). La llave puede ser elegida desde un conjunto de posibles valores, llamados el espacio de las claves o conjunto de claves. El espacio de las llaves a menudo es enorme, entre más grande mejor. La seguridad de estos algoritmos yace enteramente en la llave secreta y no en sus secretos internos. De hecho los algoritmos por sí mismos son públicos y son extensamente analizados para detectar posibles debilidades.

El principio de los cifradores codificados es presentado en la siguiente figura:

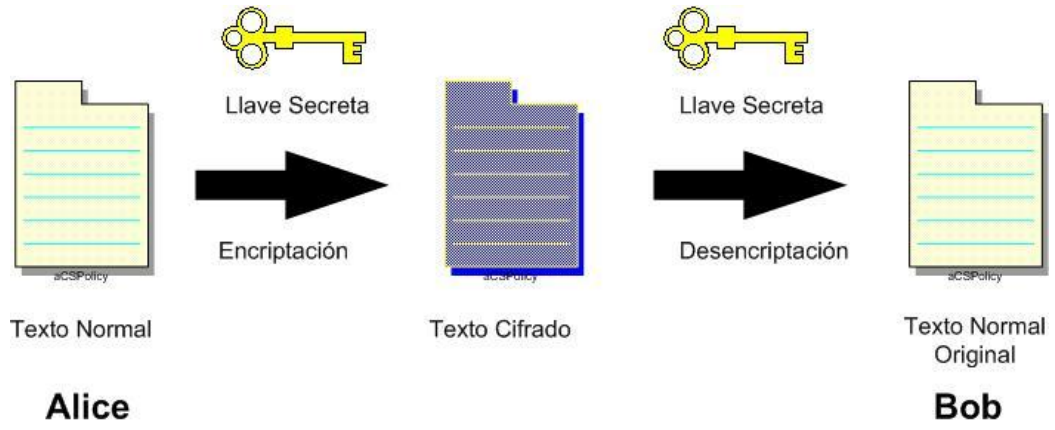


Figura 9.1. Encriptación y desencriptación utilizando la llave secreta.

9.4 AUTENTICACIÓN, INTEGRIDAD Y NO RECHAZO

La encriptación provee confidencialidad a los mensajes. Cuando existe una comunicación a través de un medio no seguro, como lo es el Internet, además de la confidencialidad es necesario:

- **Autenticación:** en un método para verificar que el emisor del mensaje es en realidad quien se supone que debería ser. cualquier intruso haciéndose pasar por alguien más es detectado por la autenticación.
- **Chequeo de integridad:** es un método para verificar que el mensaje no ha sido alterado a lo largo del camino de la comunicación. Cualquier mensaje alterado enviado por un intruso es detectado por el método de chequeo de integridad. Como un efecto adicional, errores en la comunicación son también detectados.
- **No rechazo:** es la posibilidad de probar que el emisor en realidad ha enviado el mensaje. Cuando se usan los algoritmos que proveen el método de no rechazo, el emisor no es capaz de negar posteriormente el hecho de que este en realidad envió el mensaje en cuestión.

9.5 CRIPTOGRAFÍA EN COMUNICACIONES DE RED.

Proteger una conversación de red es casi tan fundamental como realizar una, la parte de la protección viene de la necesidad de enviar datos sobre una red pública desconocida. Esto es comúnmente referido como el problema de “transmisión sobre un canal inseguro” y es casi siempre resuelto por dos métodos.

La solución más fácil, por supuesto, hacer el canal seguro al privatizar el medio. Si se asegura que terceras partes no tienen acceso a la línea física, el querer tener acceso a la información de forma no autorizada se convierte en algo extraordinariamente difícil, por lo tanto la conexión es segura. Como es usual, este no es siempre el mejor método, por muchas razones. Es demasiado costoso asegurar un medio de transmisión completo, el cual podría no ser factible así también como impráctico el cambiar con el paso del tiempo, sin mencionar que a veces es imposible asegurar el sistema de entrega de datos para la satisfacción completa de los usuarios.

Esta es exactamente la razón porque las redes privadas virtuales (VPN) serán desplegadas a gran escala en los años venideros. Desde que la solución no es privatizar un sistema de entrega de datos existente, esta debe ser la de asegurar los

datos en un canal inseguro. En otras palabras, hacerla accesible para todos, pero transformarla de alguna forma (criptografía) para que solamente la persona autorizada pueda utilizarla.

9.6 EN REALIDAD ¿QUE TAN SEGURO ES EL ALGORITMO CRIPTOGRÁFICO?

Dado el explosivo crecimiento anual en el poder de recursos de computación, los datos almacenados en formas encriptadas son más y más inseguros. La vida de una pieza particular de datos encriptados o aún la vida de un algoritmo de encriptación por sí mismo están gobernadas cruelmente por el poder de procesamiento que puede ser utilizado en contra de éste. Entre más grande es la velocidad del microprocesador, más grande es la amenaza y más rápido caen los datos en un simple ataque fuerte.

9.7 USO DE CRIPTO-SISTEMAS Y AUTENTICACIÓN EN VPN

Como en todas las comunicaciones seguras, todos los sistemas de protección tienen tres funciones importantes en común. Las comunicaciones seguras primero protegen los datos en tránsito para que las terceras partes hostiles o curiosas en medio del camino no sean capaz de interceptar y leer la transmisión (este es el concepto de *encriptación*). Entre las técnicas más populares de encriptación usadas en VPN se incluyen DES, Triple DES, RC2 y RC4.

Segundo, ambas partes deben saber con confianza que están hablando el uno con el otro, en otras palabras, Alice esta segura de que esta hablando con Bob, y viceversa, aún cuando no se puedan ver el uno con el otro (esta es el área de la *autenticación).*

Por último, ambos Alice y Bob necesitan se capaces de detectar si alguna tercera parte esta tratando de sabotear los mensajes, tanto para un fin destructivo (como la inserción de mensajes para evitar que alice pueda comunicarse con bob) como un

ataque sin daños (como la inserción de basura infrecuente para comprobar una hipótesis). Este es el concepto de *integridad del mensaje (message integrity)*, y es a veces referido como un *extracto de mensaje (message digest).* Como los es MD5 o SHA.

Estos conceptos pueden ser ilustrados mediante el siguiente ejemplo:
Cuando bob quiere enviar un mensaje a alice, bob primero implementaría una función llamada message digest a su texto normal que produciría un código hash o código de autenticación de mensaje (MAC code). El cual sería encriptado con su propia llave privada, ahora incluida en el mensaje mismo, luego todo el mensaje sería encriptado con la llave publica del receptor. Después de la transmisión, el receptor desencriptaría el paquete entero con su propia llave privada, calculará su propio código MAC desde el documento actual de texto normal, desencriptar el código MAC del emisor con su propia llave publica, entonces comparara el código MAC que localmente ha calculado con el que ha sido enviado a través de la transmisión, si difieren, el ataque ha ocurrido.
El protocolo SKIP de Sun es una implementación bastante popular de encriptación y autenticación comparable con el estándar IPSec. SKIP está disponible a través de varios vendedores para sistemas operativos Unix así también para Windows. Cada cliente que utiliza SKIP mantiene una lista de control de acceso especificando desde que clientes esta dispuesto a recibir tráfico y que tipo de encriptación utilizar con cada uno de ellos. Cuando un paquete IP es enviado desde un cliente SKIP hacia otro, el emisor encripta el paquete con el protocolo SKIP y luego es superpuesto en otro paquete IP para que pueda transitar a través del Internet.

La clave para utilizar un intercambio de datos privado ó un almacén de datos seguro depende en ser capaz de dejar fuera las personas no autorizadas y colocar cajas de seguridad alrededor de lo que se desea proteger. Sin firewalls, una VPN podría existir, si bien sin la misma filosofía de seguridad. Pero, sin encriptación, una VPN ciertamente no podría existir. Rutinas de cifrado resuelven el problema fundamental de asegurar la comunicación a través de un canal inseguro en un ambiente hostil.

9.8 ALGORITMOS CRIPTOGRÁFICOS

En el siguiente apartado se cubrirán los tres tipos básicos de algoritmos de encriptación que pueden ser usados para proteger los datos. Algunos de estos tres sistemas son inadecuados para una VPN ó presentan problemas de administración, así también, otros parecen como si fueron hechos exactamente para la protección de comunicaciones de red.

9.8.1 Algoritmos hash

Los algoritmos hash también conocidos como compendios de mensajes o solamente hashes de una sola vía (one-way), toman una cadena larga arbitraria y matemáticamente la convierten en una cadena de longitud fija. Los hashes son típicamente utilizados para verificar la validez de un mensaje en particular o una clave. Un buen escenario es uno donde un sistema necesita ser capaz de verificar la autenticación de un usuario en particular, pero no se quiere almacenar una clave no encriptada en un disco. Al hacer esto se comprometería la seguridad para cada usuario del sistema completo al mismo tiempo. Cuando el sistema aplica la función hash a la clave y luego este hash es almacenado, si el atacante que ha ganado acceso a este archivo de la clave no puede utilizarlo porque se le es imposible descifrarlo. Pero, el atacante puede realizar ataques fuertes en contra de todos los usuarios de una sola vez, esto da una razón adecuada al administrador del sistema para mantener el archivo de claves tan seguro como sea posible.

El proceso para realizar la función hash debe ser rápida, confiable y debe producir un resultado que es fundamentalmente imposible de revertir. Porque hay una pérdida de datos en la producción de la función hash (por ejemplo, la transformación de un número potencialmente largo en un número fijo más pequeño), un cripto analista tiene solamente las herramientas de ataques de fuerza bruta (o ataques fuertes), ingeniería social o algoritmos específicos para ataques. Es posible por lo tanto tener mas de un valor de entrada en la cual las funciones hash pueden tener el mismo

resultado. Un algoritmo robusto hace impensable computacionalmente hablando encontrar dos valores semejantes con mucha facilidad.

9.8.2 Sistemas de llaves secretas

Los sistemas de encriptación de llaves secretas toman como entrada un mensaje de longitud variable y una llave secreta por la cual el mensaje es transformado en un texto cifrado. De hecho, en cierto punto la transformación es bastante similar a la de los algoritmos hash. Una distinción importante es que una variable controlada por el usuario es suministrada para ayudar a encriptar los datos. Además, donde los algoritmos hash crean un resultado de longitud fija desde una variable de longitud variable, los sistemas de llaves secretas operan en bloques fijos sucesivos de entrada usando una llave de longitud fija para producir un resultado de longitud variable. Algoritmos hash son de un solo camino de encriptación (one-way) y los sistemas de llaves secretas preservan entero el texto original por lo tanto este texto original puede ser utilizado cuando sea necesario. Debido a que la llave secreta es usada en la ecuación y ésta es de longitud fija, usando una llave que es demasiado pequeña reduce por completo la seguridad del sistema. Imaginen el uso de una llave de longitud de un byte (8 bits); no debería tomar mucho tiempo a un cripto-analista el poder recorrer las 256 posibles llaves que podrían ser utilizadas para desencriptar los datos.

Desde la operación de encriptación los mensajes usan bloques de longitud fija como entrada, usando un bloque de mensaje del tamaño de un byte podría también ser inseguro debido a que los crackers solamente tendrían que crear una tabla de texto original para pares de texto cifrado, una vez que sepa que el podría mandar sus propios datos a través del algoritmo. Como con los sistemas hash, el sistema de llave secreta esta diseñado para tomar como entrada un texto original de longitud variable y producir una salida aleatoria de tamaño similar. Además, cambiando la entrada en un solo bit debería cambiar la salida por lo tanto no hay manera de rastrear una transformación desde un bit a otro bit. La aleatoriedad de los mensajes cifrados

sugiere que en algún tiempo dado, alrededor de la mitad de todos los bits en la secuencia resultante están activados (1) y la otra mitad esta desactivada (0).

La criptografía de llaves secretas usa algoritmos que efectivamente dispersan los bits completamente a través de la salida resultante y luego los mezclan al combinarlos varias veces por lo tanto se convierte en algo imposible el rastrear un bit dado a través del proceso y tener una idea de lo que le sucedió a este bit por todo el camino. Típicamente, durante el proceso de encriptación, hay muchas operaciones que pueden ser encontradas en uso incluyendo la sustitución de bits de entrada por otros bits de entrada y entonces intercambiar la posición de unos bits por la posición de otros bits.

9.8.3 Sistemas de llaves públicas

Los sistemas de llaves públicas por otro lado, son una colección de algoritmos cifradores que realizan diferentes cosas. Algunos realizan firmas digitales, algunos realizan intercambio de llaves, algunos realizan autenticación pero no encriptación y otros lo realizan todo. Sin embargo, todos ellos tienen un concepto general en común: hay siempre dos componentes que son usados para la operación en los datos de entrada. Uno de los componentes es una pieza *privada* y la otra es llamada una pieza *pública.*

Una cosa interesante de la trivialidad es que es irrelevante cual pieza actual (pública ó privada) es cual matemáticamente hablando, debido a que las dos son operaciones inversas de una con la otra.

El punto de separar las dos es que la pieza “privada” es la parte que es secreta internamente, mientras que la otra (pieza “pública” es distribuida externamente). Distribuir ambas piezas sería como regalar tu llave secreta con cada bit de información encriptado que es enviado.

9.9 ALGORITMOS DE ENCRIPTACIÓN

Estos algoritmos utilizan algoritmos matemáticos complejos para convertir texto normal en texto cifrado. Texto normal se refiere a los datos que no han sido encriptados y son fáciles de leer. Texto cifrado se refiere a los datos que han sido convertidos en formato no legible después de la encriptación. Una llave es necesitada para convertir el texto cifrado al formato de texto normal legible. Esta transformación es realizada por los algoritmos de encriptación.
Entre los algoritmos que son utilizados para la encriptación de datos en una VPN tenemos:

- Diffie-Hellman
- Rivest Shamir Adleman (RSA)
- DES
- Secure Hash Algorithm (SHA-1)
- Message Digest (MD5)
- Keyed-Hash Message Authentication Code (HMAC)

9.10 USO DE LAS LLAVES SIMÉTRICAS CON IPSEC

Estos algoritmos son utilizados en el protocolo ESP de la estructura del protocolo IPSec. Las especificaciones actuales requieren solamente DES en modo CBC, pero triple-DES y CDMF están también siendo utilizados. También existen especificaciones para el uso de IDEA (International Data Encryption Algorithm) y algunos otros algoritmos de encriptación, sin embargo el soporte para todos estos algoritmos no está extendido.

Hay dos variantes de DES en modo CBC que son utilizadas con el protocolo ESP:

- **DES-CBC con un vector de inicialización de 64-bits:** la cabecera del protocolo ESP lleva completo el vector de inicialización. Esta variante está marcada como DEC_CBC_8 en los productos IBM.
- **DES-CBC con un vector de inicialización de 32-bits:** la cabecera del protocolo ESP solamente lleva un valor de 32-bits como vector de inicialización, desde el cual el vector de inicialización completo de 64-bits es generado por la concatenación del vector de inicialización original de 32-bits y su complemento. Esta variante se puede encontrar como DES_CBC_4 en los productos IBM.

No hay una diferencia significante en los niveles de seguridad de estas variantes, DES_CBC_8, es ligeramente más grande. La mayoría de las implementaciones, por ejemplo firewalls IBM, usan vectores de inicialización secuenciales.

9.11 USO DE LAS LLAVES ASIMÉTRICAS CON IPSEC

IPSec utiliza algoritmos asimétricos para asegurar la generación de llaves y la autenticación. Estas operaciones son típicas de la estructura ISAKMP/Oakley. Ambas involucran el uso de algoritmos modulares.

a. Algoritmos de llave pública RSA.

RSA es utilizado en la estructura ISAKMP/Oakley como uno de los posibles métodos de autenticación. El principio del algoritmo RSA es el siguiente:

- tomar dos primos grandes, p y q.
- encontrar el producto n = pq; n es llamado el módulo.
- escoger un número e menor que n y relativamente primo a (p-1) (q-1), lo cual significa que e y (p-1) (q-1) no tienen otro factor común que 1.
- encontrar su inverso, d mod (p-1) (q-1), lo cual significa que ed = 1 mod (p-1) (q-1), e y d son llamados los exponentes públicos y privados, respectivamente.

La llave pública es el par (n,e); la llave privada es d. Los factores p y q deben ser mantenidos en secreto o destruidos.

b. Intercambio de llave Diffie-Hellman

El intercambio de llave Diffie-Hellman es un componente crucial de la estructura ISAKMP/Oakley. En la fase más temprana de una sesión de negociación de llave donde no hay un canal seguro establecido. Las partes obtienen las llaves secretas compartidas usando el algoritmo Diffie-Hellman. Estas llaves serán utilizadas en los siguientes pasos del protocolo de negociación de llave.

La descripción del algoritmo es el siguiente:

1. Las partes (alice y bob) comparten dos valores públicos, a modulo m y un entero g, m debería ser un número primo grande.
2. alice genera un número aleatorio grande a y realiza la operación:
   X = ga mod m
3. bob genera un número aleatorio grande b y realiza la operación:
   Y = gb mod m
4. alice envía X hacia bob
5. bob realiza la operación:
   K1 = Xb mod m
6. bob envía Y hacia alice
7. alice realiza la operación:
   K2 = Ya mod m

Ambas K1 y K2 son iguales a gab mod m. Esta es la llave secreta compartida. Ninguna de las partes es capaz de generar este valor sin conocer a o b. La seguridad del intercambio esta basado en el hecho de que es extremadamente difícil invertir la exponenciación realizada por las partes.

9.11.1 Funciones hash

Las funciones hash son fundamentales para la criptografía. Una función hash es una función que toma un dato de entrada de longitud variable y produce datos de salida de longitud fija (el valor hash), el cual puede ser apreciado como la huella digital de la entrada. Eso es, si los valores hash de los dos mensajes combinan, entonces se tiene un alta certeza de que los mensajes son los mismos.

Criptográficamente, las funciones hash útiles deben ser de un solo sentido, lo cual significa de que deberían ser fáciles de calcular, pero imposibles de revertir. Un ejemplo cotidiano de una función de un solo sentido es hacer puré una papa; es fácil de realizarlo, pero una vez hecho el puré, reconstruir la papa original es un tanto imposible. Una buena función hash debería ser resistente a colisiones. Debería ser difícil encontrar dos diferentes entradas que lleguen al mismo valor. Como cualquier función hash que acota un conjunto de entrada hacia un conjunto de salida más pequeño, teóricamente es imposible encontrar colisiones. El punto clave es proveer una huella digital única hacia cada mensaje, que lo identifica con una alta confianza, semejante a una huella dactilar real que identifica a una persona.

Una función hash toma una llave como su segundo parámetro de entrada y la salida depende tanto del mensaje como de la llave, este resultado es llamado: Código de Autenticación de Mensaje (MAC – Message Authentication Code) como se muestra en la siguiente figura:

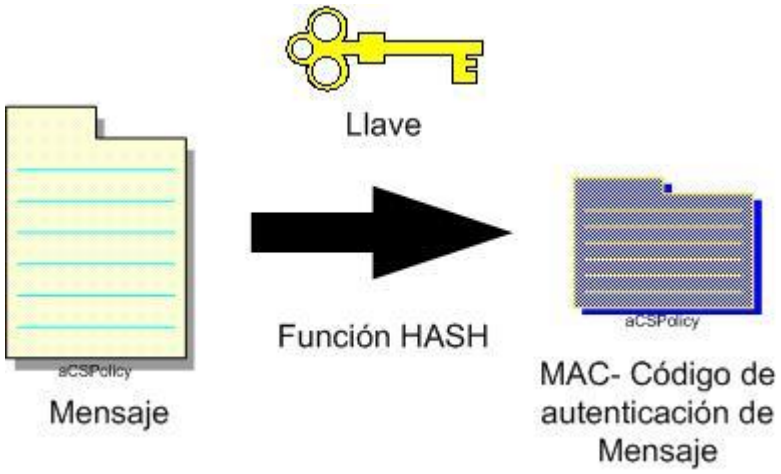


Figura 9.4. Función Hash

De manera simple, si se encripta un hash, se convierte en un MAC. Si se agrega una llave secreta al mensaje entonces la función hash la concatena, el resultado es un MAC. Tantos algoritmos simétricos como asimétricos pueden ser utilizados para generar MACs. Las funciones hash son primeramente utilizadas en el chequeo de integridad y técnicas de autenticación.

Ahora se describirá como la integridad y la autenticación está asegurada con las funciones hash:

1. el emisor calcula el resultado hash del mensaje y lo agrega al mensaje mismo.
2. el receptor calcula el resultado hash del mensaje recibido y luego compara este resultado con el resultado hash transmitido.
3. si los resultado hash combinan, el mensaje no fue corrompido.
4. en el caso de MAC donde la encriptación de la llave (simétrica y asimétrica) debería haber sido utilizada solamente por un emisor confiable, una desencriptación MAC exitosa indica que el emisor requerido y el actual son idénticos. (a menos, claro que las llaves hubiesen estado comprometidas).

La siguiente figura describe el procedimiento anteriormente descrito, la notación del mensaje y el MAC reflejan el hecho de que el mensaje podría haber sido alterado mientras cruzaba el canal inseguro.

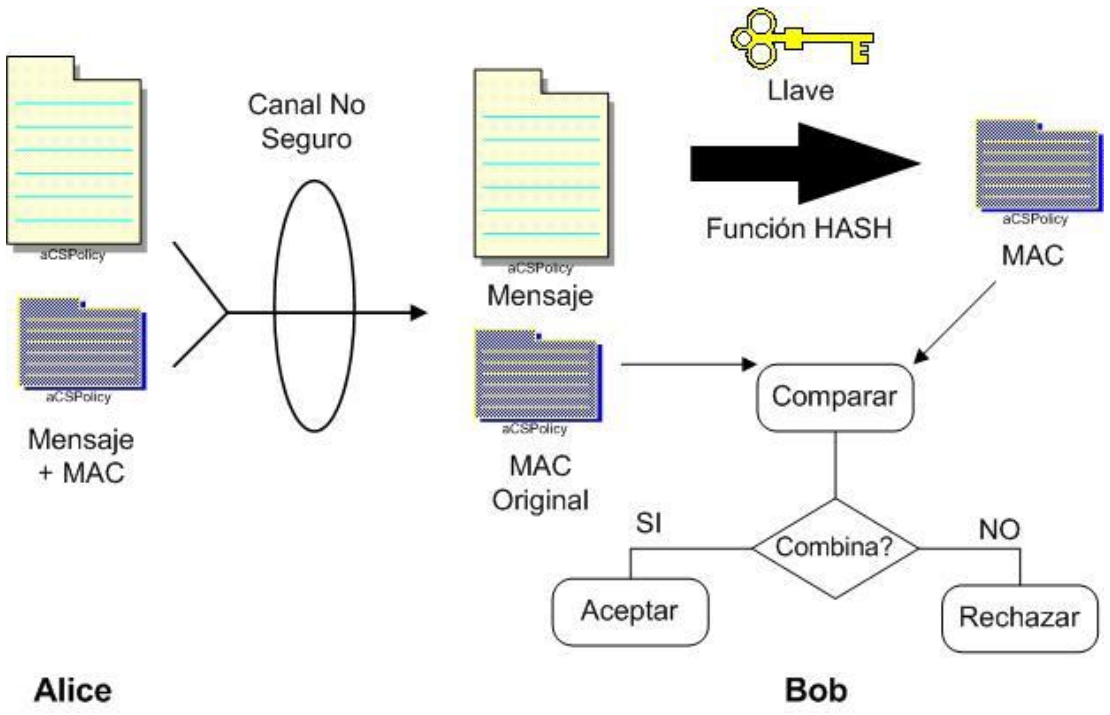


Figura 9.5. Procedimiento Hash

Cualquiera podría argumentar que el mismo resultado podría ser obtenido con cualquier clase de encriptación, porque si un intruso modifica el mensaje encriptado, la desencriptación resultaría sin sentido, además la alteración podría ser detectada. La respuesta es que muchas veces solamente la integridad y/o autenticación es necesaria, quizás con la encriptación en algunos de los campos del mensaje.

La encriptación de una función hash con una llave privada es llamada Firma Digital. Esta puede ser apreciada como un MAC especial. Utilizando firmas digitales en vez de encriptar el mensaje completo con una llave privada lleva al logro de un mejor desempeño.

La encriptación de una llave secreta con una llave pública es llamada Sobre Digital. Esta es una técnica común utilizada para distribuir llaves secretas para algoritmos simétricos.

Ejemplos de funciones hash:

Las funciones hash más ampliamente utilizadas son MD5 y SHA-1 (Secure Hash Algorithm 1). MD5 fue diseñado por Ron Rivest (co inventor de RSA). SHA-1 está altamente inspirado en MD5 y fue diseñado por NSA (National Security Agency) para el uso con DSS (Digital Signature Standard). MD5 produce una función hash de 128 bits, mientras que SHA-1 produce una función hash de 160 bits. Ambas funciones codifican el mensaje en su salida. SHA-1 es apreciado como más seguro, debido a que produce un resultado hash más largo.

9.12 ALGORITMOS ASIMÉTRICOS O ALGORITMOS DE LLAVES PÚBLICAS.

Estos algoritmos dirigen la mayor de las desventajas de los algoritmos simétricos, el requerimiento de un canal de intercambio de llave seguro. La idea es que dos diferentes llaves deberían de ser usadas: una llave pública, tal como el nombre lo indica, es conocida por todo el mundo, y una llave privada, la cual debe ser mantenida con una alta seguridad por el propietario. La llave privada no puede ser determinada desde la llave pública. Un mensaje de texto claro encriptado con la llave pública puede ser desencriptado solamente con su correspondiente llave privada y viceversa. Un mensaje de texto claro encriptado con una llave privada puede ser desencriptado solamente con su correspondiente llave pública. De esta manera, si alguien envía un mensaje encriptado con su correspondiente llave pública del destinatario, este solamente puede ser leído por el destinatario.

El proceso es mostrado en la siguiente figura, donde alice envía un mensaje encriptado a bob.

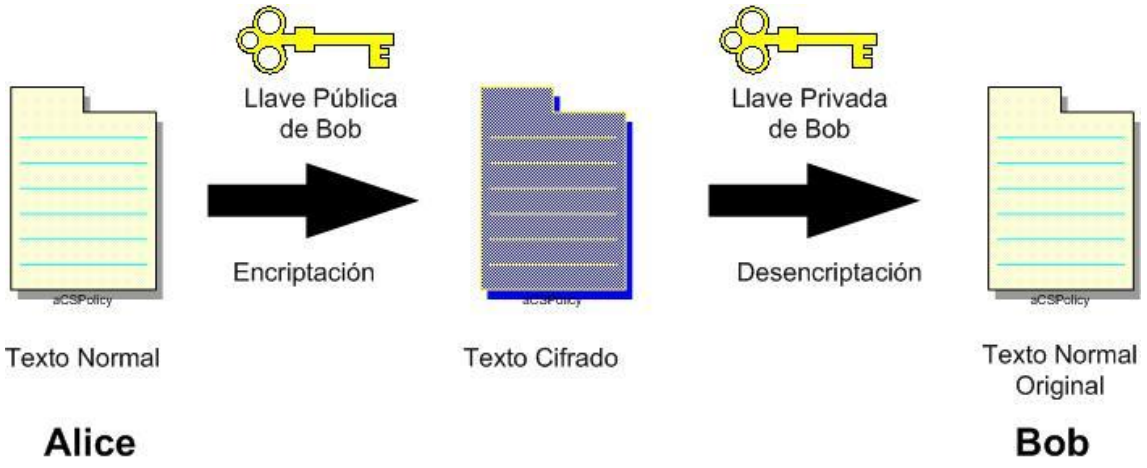


Figura 9.2. Algoritmos asimétricos

Como la llave pública está disponible para todos, la privacidad esta asegurada sin necesidad de un canal de intercambio de llaves seguro, las partes que desean comunicarse toman la llave pública del otro.

9.12.1 Autenticación y no rechazo

Una propiedad interesante de los algoritmos de llaves públicas es que pueden proveer autenticación. Se utiliza la llave privada para la encriptación. Desde que todos tienen acceso a la correspondiente llave pública y pueden desencriptar el mensaje, ésta no provee privacidad. Sin embargo, ésta llave autentifica el mensaje. Si alguien puede exitosamente desencriptar el mensaje con la llave pública requerida del emisor, entonces el mensaje ha sido encriptado con la correspondiente llave privada, la cuál es conocida solamente por el verdadero emisor. De esta manera, la identidad del emisor está verificada. La encriptación con una llave privada es usada en firmas digitales.

En la figura siguiente, alice encripta su mensaje con su llave privada, con el propósito de habilitar a bob para que verifique la autenticidad del mensaje.

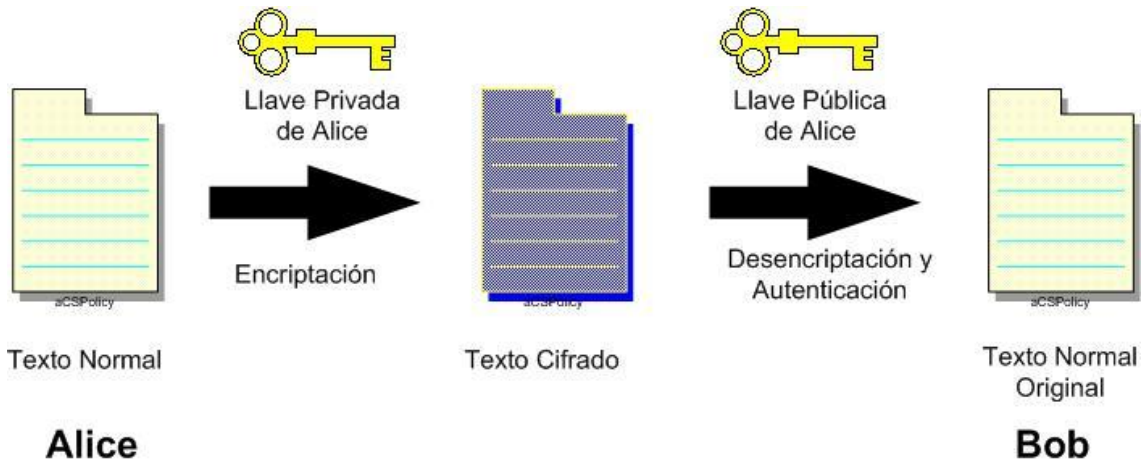


Figura 9.3. Autenticación y rechazo

Autenticación por medio de la encriptación con una llave privada.

Yendo un paso adelante, la encriptación con una llave privada da un resultado de no rechazo también. La mera existencia de tal mensaje encriptado, testifica que el emisor en realidad lo ha enviado, porque solamente el pudo haber utilizado la llave privada para generar el mensaje. Adicionalmente, si un registro de tiempo es agregado, entonces la hora y la fecha exacta pueden ser conocidas.

9.13 USO DE FUNCIONES HASH CON IPSEC:

La estructura IPSec puede usar tanto MD5 como SHA-1 para el cálculo de MAC con el fin de proveer autenticación e integridad. Hay dos maneras de utilizar cada una de las funciones, lo cual resulta en cuatro diferentes posibilidades: MD5 codificado (Keyed MD5), SHA-1 codificado (Keyed SHA-1), HMAC-MD5-96 y HMAC-SHA-1-96. Otras funciones hash pueden también ser incluidas.

9.13.1 MD5 Codificado (Keyed MD5) y SHA-1 Codificado (Keyed SHA-1)

Usar MD5 y SHA-1 en modo codificado es simple. La llave secreta compartida y el datagrama han de ser protegidos, ambos son parámetros de entrada en el algoritmo

hash y la salida de este (el valor hash) es colocado en el campo de autenticación del encabezado AH, como se muestra en la siguiente figura:

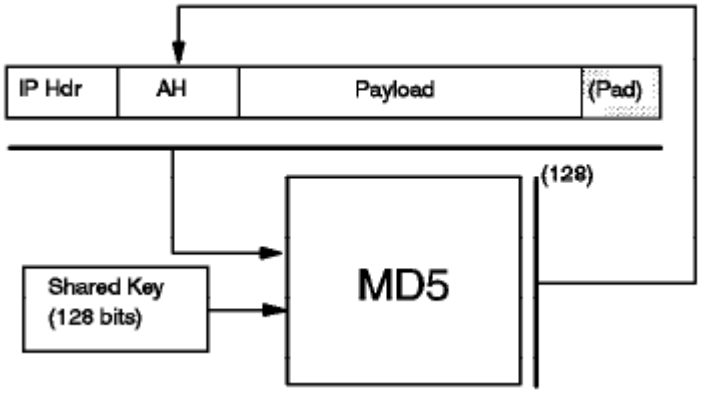


Figura 9.6. Proceso de un MD5 codificado.

SHA-1 codificado opera de la misma manera, la única diferencia es que es un valor hash de 160-bits.

9.13.2 HMAC-MD5-96 y HMAC-SHA-1-96

Un método más robusto es el “Hashed Message Authentication Code (HMAC)”, él cual fue propuesto por IBM. HMAC por sí mismo no es una función hash, sino que es una manera robusta de criptografía para usar una función hash específica para el cálculo de MAC.

Ahora se muestra como MAC trabaja, considerando MD5 como ejemplo, la función base es aplicada dos veces en la sucesión. En la primera ronda la entrada para MD5 es la llave secreta compartida y el datagrama. El valor de salida hash de 128 bits y la llave es la entrada otra vez en la segunda ronda. Los 96 bits menos significativos del valor hash resultante son usados como la MAC para el datagrama.

A continuación se presenta la siguiente figura ilustrando el ejemplo:

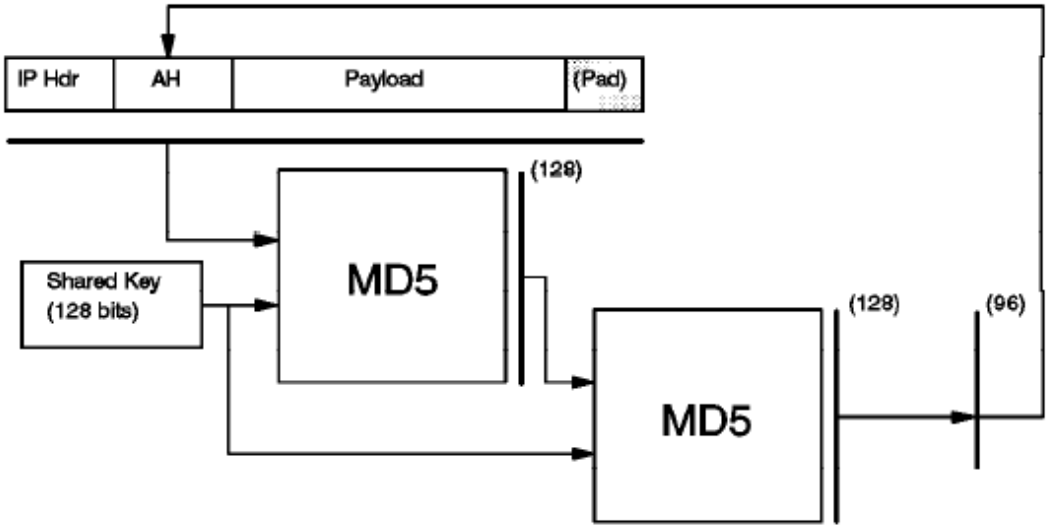


Figura 9.7. Procesamiento HMAC-MD5-96

HMAC-SHA-1-96 opera de manera similar, exceptuando que los resultados intermedios tienen la longitud de 160-bits.

9.14 DSS (DIGITAL SIGNATURE STANDARD)

Como se mencionó anteriormente, una valor hash encriptado con una llave secreta es llamado una firma digital y se ilustra con la figura siguiente:

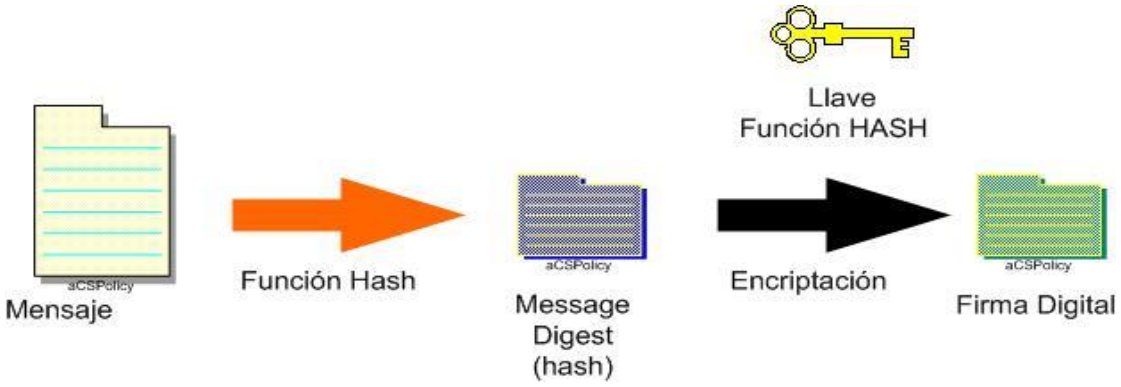


Figura 9.8. Generando una firma digital

Un método de autenticación que puede ser usado con ISAKMP/Oakley es DSS el cuál fue seleccionado por NIST y NSA para ser el estándar de la autenticación digital del gobierno de Estados Unidos.

Esquemas de autenticación y encriptación:

Una VPN implementa varios mecanismos de seguridad para asegurar la integridad y seguridad durante la transmisión. Estos procedimientos de seguridad involucran el uso de passwords, llaves secretas, algoritmos de encriptación y funciones hash.

9.15 MÉTODOS UTILIZADOS PARA ASEGURAR UNA VPN

a. Passwords

Requiere que los usuarios remotos provean la información utilizada para establecer una conexión remota. Estos passwords son usualmente mantenidos en una base de datos centralizada en la oficina corporativa central. El servidor RAS (Remote Access Server) verifica el password proporcionado por el usuario remoto en su base de datos. Los password necesitan ser cambiados frecuentemente para evitar el riesgo de que los hackers puedan ser capaces de descifrarlos. El uso de password de una sola vez aseguran un alto grado de seguridad.

b. Criptografía

Envuelve el intercambio de llaves secretas entre dos partes que quieren establecer una conexión segura. Las llaves secretas son utilizadas para decodificar información utilizada para verificar las identidades de los usuarios remotos. Llaves públicas y privadas son usadas por los algoritmos de criptografía para encriptar y desencriptar datos y asegurar un alto nivel de seguridad.

La criptografía de llaves simétricas usa una llave secreta individual para encriptar y desencritar datos en ambos lados de una conexión. Criptografía de llaves asimétricas utiliza ambas llaves una llave pública y una llave privada para encriptar y desencriptar los datos. La llave pública es intercambiada entre el emisor y el receptor y la llave privada es utilizada para desencriptar la información codificada.

La siguiente figura ilustra el intercambio de llaves secretas entre dos usuarios remotos:

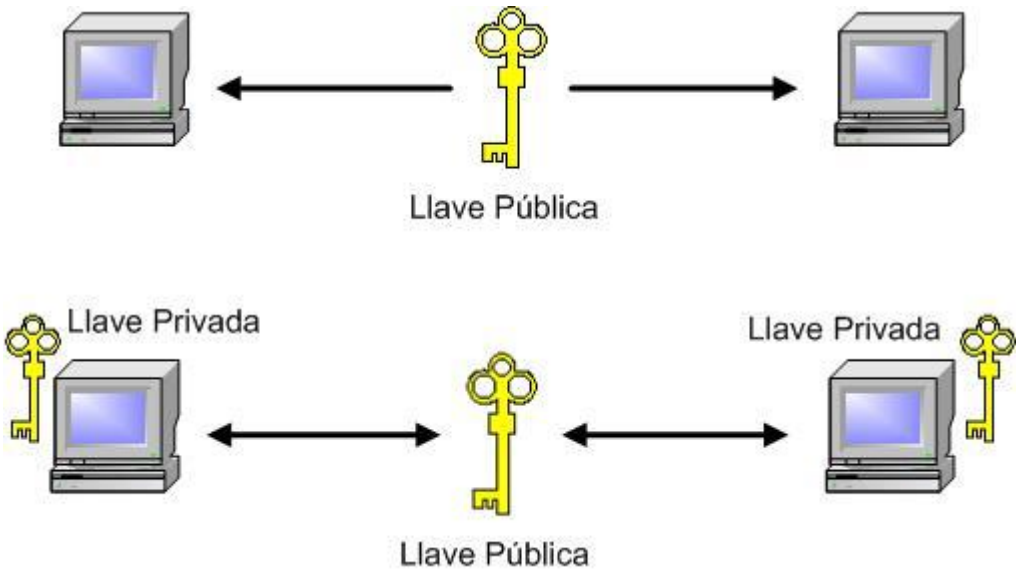


Figura 9.9. Intercambio de llaves secretas

c. Algoritmos hash

Crean una forma condensada de un mensaje o archivo de datos llamado compendio de mensaje. El uso de algoritmos matemáticos asegura que compendios de mensajes únicos son creados para cada mensaje ó archivo de datos. Un compendio de mensaje permite al receptor determinar cuando un archivo de datos ha sido atacado durante el tránsito y cuando no. El compendio de mensaje de un archivo alterado durante el transito no coincidirá con el compendio de mensaje del archivo original. En una VPN, se puede utilizar funciones hash para determinar si la información provista por el usuario remoto coincide con la información mantenida en el servidor de autenticación. La ventaja de utilizar algoritmos hash es que el archivo de datos original no puede ser deducido desde el compendio de mensaje.

Estos métodos pueden ser utilizados para establecer una VPN que provee un ambiente seguro similar al de una red privada tradicional establecida mediante el uso

de tecnologías WAN. Estos algoritmos complejos requieren de un alto poder de procesamiento y pueden tener un impacto grande en el desempeño de una VPN.

9.16 ESQUEMAS DE AUTENTICACIÓN

La preocupación primaria de una organización es asegurarse de que sus recursos corporativos están accesibles solamente para usuarios autorizados. Para lograr esto, un sistema de autenticación de usuarios remoto debe ser implementado. Una base de datos mantenida en las instalaciones principales de la corporación contiene la información necesaria, entre estas se tienen: nombre del usuario, passwords, nombres de dominio y cualquier otra información adicional que ayuda a verificar la identidad del usuario remoto.

Las peticiones de conexión son verificadas contra la información que está almacenada en la base de datos.

Los siguientes métodos son utilizados para autenticar un usuario:

9.16.1 Protocolo de autenticación de password (Password Authentication Protocol – PAP)

Involucra el uso de nombres de usuarios y passwords para autenticar una conexión de red. Usuarios remotos proveen esta información para establecer una conexión con un servidor de red. Este método no es adecuado para una VPN porque la información intercambiada entre el cliente y el servidor no está encriptada.

Provee un método de autenticación reversible bidireccional que involucra el uso de passwords encriptados. Este es usado para conectar un servidor Windows 2000 usando un RAS a una computadora remota utilizando el software cliente de Shiva.

Las conexiones entre PAP y SPAP no son usadas en una VPN porque estas son vulnerables a las amenazas de seguridad del Internet como lo son el hijacking y

ataques de personas que están escuchando la transmisión entre el receptor y el emisor.

9.16.2 Challenge-Handshake Authentication Protocol (CHAP)

Verifica la identidad de un usuario remoto usando una llave secreta compartida. Después de que el enlace ha sido establecido, el autenticador envía un mensaje referido como un desafió hacia el usuario remoto. Como respuesta, el usuario remoto envía un valor hash calculado en base a su llave secreta y una función hash. La autenticación es completada si el valor calculado enviado por el usuario remoto combina con el valor hash calculado por el autenticador utilizando la misma función hash y la llave secreta. Hay que notar que la llave secreta no es intercambiada en el enlace.

MSCHAP es una versión de Microsoft usada para autenticar usuarios remotos antes de establecer una conexión VPN.

9.16.3 Protocolo de autenticación extensible (Extensible Authentication Protocol EAP)

Permite que la autenticación de los usuarios sea desarrollada después de que el enlace inicial es establecido. EAP es una extensión del protocolo PPP (Point-to-Point Protocol), que permite el uso de varios esquemas de autenticación como lo son tarjetas inteligentes, certificados digitales y passwords. Esta función hace de EAP muy útil para la autenticación de usuarios remotos en una VPN porque se puede seleccionar de un amplio rango de esquemas de autenticación.

9.17 CERTIFICADOS DIGITALES

Proveen la opción de usar firmas digitales para verificar la identidad de los usuarios remotos. Un certificado digital usa una serie de llaves públicas y privadas para verificar la identidad de un usuario. Esta verificación es realizada por una Autoridad

de Certificado (Certificate Authority - CA), la cuál puede ser una organización por sí misma ó una organización externa. Una firma digital emitida por un CA contiene una llave pública asignada al usuario remoto y es firmada digitalmente por la autoridad que la emite. Un algoritmo de firma digital (Digital Signature Algorithm -DSA) es usado para generar y verificar firmas digitales. Al momento de la autenticación, un usuario remoto envía el certificado digital hacia el CA. La llave pública dentro de un certificado digital es comparada con la información mantenida por el CA para verificar la identidad del usuario remoto. Las llaves privadas son usadas para encriptar y desencriptar datos después de que la conexión es establecida. Entre las mayores empresas de CA se tiene: VeriSign, Thawte, ValiCert, GlobalSign y PricewaterhouseCoopers (PwC).

9.18 SEGURIDAD DE ENCRIPTACIÓN CON L2TP/IPSEC

La encriptación es determinada por el establecimiento de un modo rápido ó IPSec SA. Los algoritmos de encriptación disponibles incluyen lo siguiente:

- Data Encryption Standard (DES) con una llave de 56 bits.
- Triple DES (3DES), el cual usa tres llaves de 56 bits y está diseñado para ambientes de alta seguridad, porque IPSec fue diseñado para redes IP donde los paquetes se pueden perder o llegar fuera de orden, cada paquete IPSec es desencriptado independientemente de los otros paquetes IPSec.

Las llaves de encriptación iniciales son derivadas desde el proceso de autenticación en modo principal de IPSec. Para las conexiones encriptadas DES, nuevas llaves de encriptación son generadas después de 5 minutos o 250 MB de datos transferidos. Para las conexiones encriptadas 3DES, nuevas llaves de encriptación son generadas cada hora o 2 GB de datos transferidos.

9.19 SEGURIDAD DEL FILTRADO DE PAQUETES

Un servidor VPN es un enrutador IP, reenviando paquetes IP entre interfaces (adaptadores de red o interfaces lógicas). Esto lo hace una entidad muy poderosa en la red, este puede propagar y enrutar tráfico hacia potencialmente cualquier lugar en la Intranet o hacia la Internet si las debidas precauciones de seguridad no son tomadas. Para proveer seguridad, un enrutador IP puede permitir o no permitir el flujo de tipos muy específicos de trafico IP. Esta capacidad, llamada filtrado de paquetes IP, provee una manera para que el administrador de red pueda definir precisamente que trafico IP es recibido y enviado por el enrutador. El filtrado de paquetes IP es un elemento de conexión importante para las Intranets corporativas para poder conectarse a la red pública como lo es el Internet.

El filtrado de paquetes IP consiste en la creación de una serie de definiciones llamados filtros, los cuales definen al router que tipo de tráfico es permitido o no permitido en cada interfaz. Los filtros pueden ser configurados para tráfico entrante o saliente.

- Filtros de entrada, definen que tráfico entrante en la interfaz del router está permitido a enrutar o procesar.
- Filtros de salida, definen que tráfico el router está permitido a enviar desde su interfaz.

Sin el establecimiento de filtros de paquetes para el tráfico PPTP y L2TP/IPSec, el servidor VPN es vulnerable a varios tipos de ataques de negación de servicios (DoS) y porque el servidor VPN es un router puede ser posible para un atacante en el Internet acceder directamente a los recursos privados de la Intranet. Los filtros de paquetes pueden imposibilitar cualquier conexión no autorizada y mantener la integridad de los recursos internos al cortar el acceso a los recursos no autorizados.

9.20 SEGURIDAD DE AUTENTICACIÓN

Las credenciales de seguridad toman tanto la forma de nombre de usuario y password como de un certificado. Si se utiliza el apropiado protocolo de seguridad de autenticación se puede asegurar que las partes confidenciales de las credenciales (como los passwords ó la llave privada para un certificado) nunca son enviadas. Más bien, los clientes VPN que se conectan proveen la prueba del conocimiento de las credenciales confidenciales.

9.21 SEGURIDAD DE AUTENTICACIÓN PARA CONEXIONES L2TP/IPSEC

La autenticación para las conexiones L2TP/IPSec ocurren en dos diferente niveles: la computadora es autenticada y el usuario es autenticado. Esto permite al túnel IPSec el ser establecido primeramente en la fase de autenticación antes de que la conexión sea hecha, además permite que todas las comunicaciones se realicen en un estado encriptado.

Fase Uno: la autenticación de la computadora IPSec junto con la autenticación de la computadora VPN del cliente y el servidor VPN es realizada cuando se establece una asociación de seguridad IPSec-ESP a través del intercambio de la computadora, también conocida como certificados de la “máquina”. La negociación en modo principal y modo rápido IPSec se lleva a cabo y las asociaciones de seguridad IPSec son establecidas con un algoritmo de encriptación acordado, un algoritmo hash y las llaves de encriptación. Para usar L2TP en IPSec, un certificado de la computadora “máquina” debe ser instalado en ambos tanto en el cliente VPN como en el servidor VPN.

Fase Dos: la autenticación de nivel de usuario L2TP ahora que el túnel IPSec está establecido y todo esta sucediendo en un modo encriptado, el usuario que intenta la conexión L2TP es autenticado usando los protocolos de autenticación de usuario basado en PPP como lo son: EAP, MS-CHAP, CHAP y PAP. Porque IPSec encripta

los procesos de establecimiento de conexión PPP cualquier método de autenticación PPP puede ser usado aún PAP, el cuál pasa la información de forma clara por lo tanto ahora está protegida por IPSec. Sin embargo, el uso de MS-CHAP v2 ó EAP-TLS es altamente recomendado porque estos proveen autenticación mutua. Desde que la infraestructura de un certificado fue requerida para proveer certificaciones para las maquinas debería ser simple el proveer certificaciones para los usuarios también, vía auto enrolamiento del Active Directory de Windows 2003 y también tomar en cuenta el alto nivel de autenticación con los certificados.

9.22 SEGURIDAD DE AUTORIZACIÓN

La autorización es la verificación de que el intento de conexión está permitido. La autorización ocurre después de una autenticación exitosa. Para que un intento de conexión sea aceptado, el intento de conexión debe ser tanto autenticado y autorizado. Es posible que el intento de conexión sea autenticado mediante el uso de credenciales válidas pero no está autorizado. Usualmente esto es porque el Active Directory conoce que el individuo perteneciente al grupo no tiene el derecho para acceder a la red VPN. Ejemplo de esto pueden ser contratistas o empleados de medio tiempo que no deberían tener acceso a la información a menos que estos fueran monitoreados como empleados de tiempo completo. Otro ejemplo puede ser con implementaciones internas para la VPN donde solo los miembros del departamento de recursos humanos pueden acceder a la información en la red protegida. En este caso, el intento de conexión es denegado.

CAPITULO 10. PROTOCOLOS UTILIZADOS EN LAS VPN

Describe la forma de crear un túnel, que tipo de tecnologías existen y las ventajas que ofrece cada una de ellas. Los protocolos de túneles son componentes muy importantes para cifrar, autenticar y transportar la información que viaja por un medio inseguro como lo es el Internet. La estrategia “defensa en profundidad” necesita de estos niveles de seguridad para poder ser efectiva cuando un intruso quiere violar la red.

Puntos clave

- Métodos para crear un túnel VPN
- Describe cada una de las tecnologías que existen para crear un túnel VPN.
- Menciona la estructura de cada tecnología de túnel para VPN
- Describe como ayuda cada tecnología de túnel VPN a la estrategia de seguridad defensa en profundidad
- Ventajas y desventajas de cada tecnología.

10.1 EL TÚNEL

Mientras que los costos de la eficacia de las VPN son atribuidos al uso de la Internet, la seguridad y el resultado de la seguridad que ofertan las VPN al hacer un túnel. Es necesario describir las bases que constituyen una tecnología de túnel y el papel que juegan para asegurar la seguridad entre redes corporativas. Además sobre los tipos diferentes de túneles y los protocolos que construyen túneles.

10.1.1. Entendiendo la tecnología de túnel.

Un túnel es el componente más significativo de la tecnología de VPN. Permite que las organizaciones elaboren redes virtuales a través del Internet y en otras redes públicas. Esta red virtual no puede ser alcanzada por los intrusos, los usuarios o las computadoras que no son parte del la Intranet de la organización. La red intermedia comúnmente usada es el Internet. Sin embargo, cualquier otra red pública o red privada puede servir como una red intermedia durante una transmisión de datos.

La técnica de elaboración de un túnel para encapsular un paquete entero de datos en un formato pequeño es creada por un protocolo. Es decir el encabezado del protocolo de túnel es adicionado al paquete original. El paquete resultante es transferido al nodo o a la red destino a través de la infraestructura intermedia.

El aspecto más importante de hacer un túnel es que el paquete original de los datos, también referido como paquete de carga (payload), puede pertenecer a un protocolo sin apoyo. En lugar de transferir el paquete original, el cual no puede ser encaminado a través de la infraestructura intermedia, el protocolo de túnel añade un encabezado de paquete de túnel. Este encabezado proporciona la información de encaminamiento indispensable para poder entregar con éxito el paquete a través de la red interna.

Cuando un túnel encamina un paquete al nodo destino, él viaja por medio de la red interna a través de una trayectoria lógica. Esta trayectoria lógica se refiere como

túnel. Cuando el paquete de túnel es recibido el paquete vuelve a su formato original.

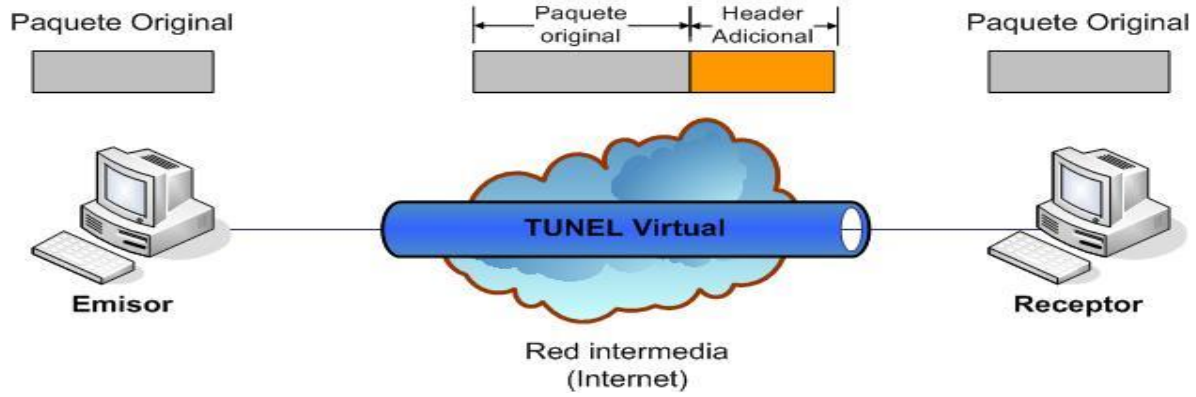


Figura 10.1 Proceso de un túnel.

10.1.2. Las ventajas de la tecnología de túnel.

Construir un túnel ofrece un número de ventajas que se detallan a continuación:

- **Simplicidad y facilidad de la puesta en práctica.** la idea básica de elaborar un túnel es simple, la propia tecnología es fácil de poner en práctica. Por otra parte, no hay necesidad de cambiar la infraestructura existente para acomodar la tecnología. Al crear un túnel es una solución viable y lucrativa para las organizaciones.
- **Seguridad**. El acceso al túnel de una organización es prohibido para usuarios no autorizados. Como consecuencia, el viaje de los datos por el túnel es relativamente seguro a pesar del hecho que los datos se están transmitiendo a través de un medio inseguro y publico, tal como es el Internet.
- **Rentabilidad.** La tecnología de túnel utiliza redes públicas como Internet. Estas redes trabajan para transferir datos a su destino. Esto hace que un túnel sea una solución extremadamente rentable, especialmente cuando se compara con el costo de implementación de las Intranet privadas que atraviesan el globo por medio de líneas arrendadas. Además, una organización puede ahorrar una cantidad considerable de dinero que tendría que gastar anualmente en la administración y el mantenimiento de estas soluciones costosas.

- **Indiferencia del protocolo.** Los datos que pertenecen a los protocolos no ruteables, tales como Network Basic Input/Output System (NetBIOS), y NetBIOS Enhanced User Interface (NetBEUI) no son compatibles con los protocolos TCP e IP del Internet. Por lo tanto, estos paquetes de datos no pueden ser encaminados a través del Internet. Sin embargo, al elaborar un túnel permite que los paquetes no IP sean enviados con éxito al destino envolviéndolos dentro de paquetes IP.
- **Ahorro de direcciones IP.** Al elaborar un túnel permite que los protocolos con las direcciones no ruteable y no IP sean insertados dentro de un paquete que utilice una dirección IP pública global. Consecuentemente, en vez de tener que comprar y asignar una dirección IP global para cada nodo dentro de la red, la organización puede comprar un bloque pequeño de direcciones IP. Cuando un nodo dentro de esta red privada establece una conexión de VPN, cual quiera de las direcciones disponibles del bloque de IP se pueden añadir a los paquetes de los datos no-IP. Así, la red privada puede reducir la necesidad de una organización de adquirir direcciones IP.

10.1.3. Los componentes de un túnel.

Para establecer con éxito un túnel de comunicación entre dos extremos, se necesitan cuatro componentes los cuales son:

- **Red objetivo.** La red que contiene los recursos que necesitan ser accedidos por el cliente remoto,
- **Nodo iniciador.** El cliente remoto o servidor que inician las audiencias de VPN. El nodo iniciador puede ser una red local o un usuario móvil usando una computadora portátil
- **HA (Home Agent).** La interfaz del software reside generalmente en el nodo de acceso de la red objetivo (router). Sin embargo, un nodo de destinación, tal como un servidor de acceso dial-up, puede también recibir el HA. El HA recibe y autentica las peticiones entrantes de verificar acerca de cuales son

los host de confianza. Sobre la autentificación acertada del host, el HA permite el establecimiento de un túnel.

- **FA (Foreign Agent).** La interfaz de software reside en el nodo del iniciador o en el nodo de acceso de red a la cual el nodo del iniciador pertenece (router). El nodo iniciador utiliza el FA para solicitar una sesión VPN al HA de la red objetivo.

10.1.4. Operaciones del túnel.

Las operaciones de la tecnología para elaborar un túnel se pueden dividir en dos fases:

- Fase uno. El nodo del iniciador o el cliente remoto solicita una sesión VPN y es autenticado por el HA correspondiente.
- Fase dos. La transferencia de datos real ocurre a través del túnel.

En la fase uno se inicia una petición de conexión y se negocian los parámetros de la sesión. (Esta fase se puede también referir como la fase del establecimiento del túnel.) Si se negocia con éxito la petición y los parámetros de la sesión, entonces la comunicación en el túnel es establecida entre los dos extremos. Esto ocurre de la manera siguiente:

- El iniciador envía la petición de conexión al FA situado en la red.
- El FA autentica la petición validando el nombre de usuario y su contraseña. El FA utiliza generalmente los servicios de un servidor Remote Access Dial-Up Services (RADIUS) o un Terminal Access Controller Access Control Service (TACACS) para autenticar la identidad del nodo del iniciador.
- Si el nombre de usuario en el sistema y la contraseña suministradas por el usuario no son validos, la solicitud para las audiencias de VPN es rechazada. Sin embargo, si el FA autentica la identidad del iniciador con éxito, transmite a la petición a HA de la red objetivo.
- Si la petición es aceptada por el HA, el FA le envía la identificación cifrada del nombre del usuario y la de contraseña correspondiente.

- El HA verifica la información suministrada. Si la verificación es acertada, el HA envía la contestación del registro, junto con un número de túnel, al FA.
- Se establece un túnel cuando el FA recibe la contestación del registro y el número del túnel.

Nota: si los dos extremos no utilizan el mismo protocolo al hacer un túnel, las variables de la configuración del túnel tales como cifrado, los parámetros de la compresión, y el mecanismo del mantenimiento del túnel son también negociados.

Con el establecimiento del túnel, la fase I se considera terminada y la fase II, o la fase de transferencia de datos, comienza. Las transacciones en la fase de transferencia de datos ocurren de la siguiente manera:

- El iniciador inicia enviando los paquetes de los datos para la FA.
- La FA crea el encabezado del túnel y los añade a cada paquete de datos. La información del encabezado del protocolo routable (que fue negociado en la fase I) se añade al paquete.
- El FA envía el paquete cifrado de los datos que resulta del HA usando el número del túnel
- Al recepcionar la información cifrada, el HA quita el encabezado del túnel y el encabezado del protocolo routable, de esta manera extrae el paquete de nuevo a su formato original.
- Los datos originales se remiten al nodo destino previsto en la red

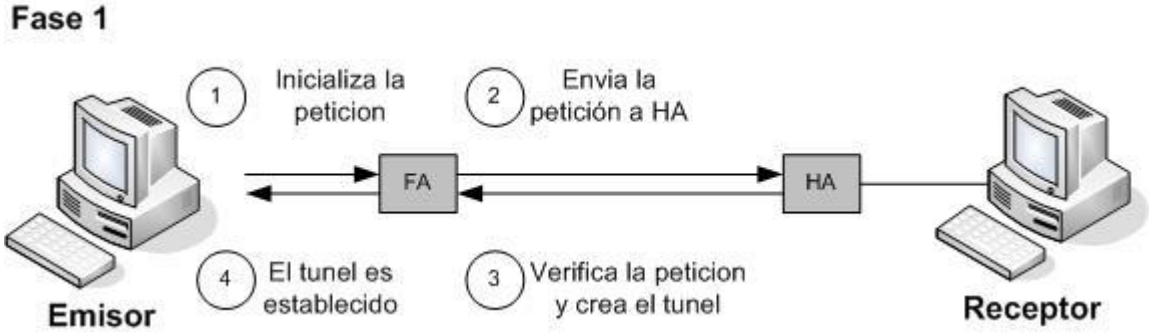


Figura 10.2 Proceso para establecer un túnel.

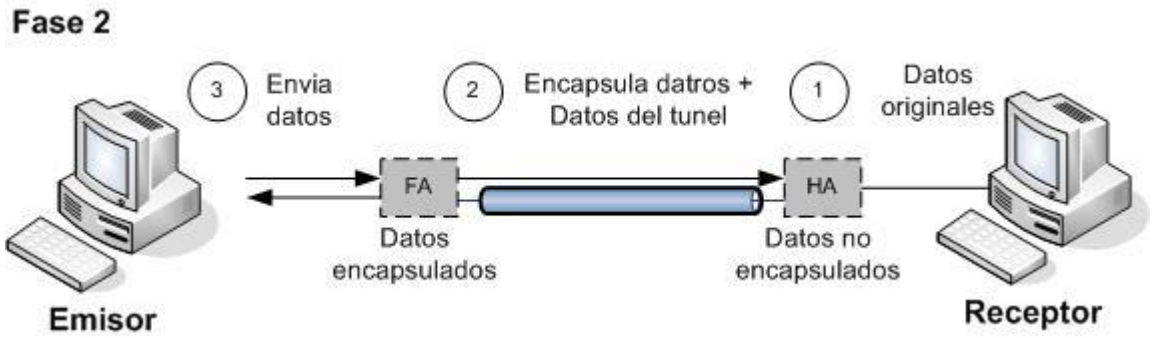


Figura 10.3 Proceso de transferencia en un túnel.

10.1.5. Formato de un paquete de túnel.

Antes de entregar el paquete original de datos a la red objetivo a través del túnel, Este es cifrado por la FA. El paquete cifrado es llamado como: paquete de túnel el cual se muestra su formato a continuación. En la siguiente figura10.4 se muestra el formato de un paquete de túnel.

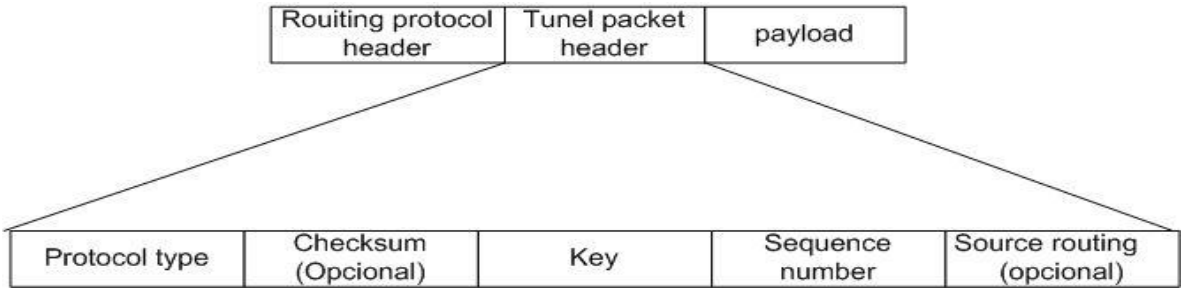


Figura 10.4 Formato del paquete de dato.

- Rouiting protocol header. Este campo de encabezado contiene las direcciones de la fuente (FA) y el destino (HA). Este encabezado es generalmente el encabezado estándar IP.
- Túnel packet header. Este encabezado contiene los cinco campos siguientes:
    - Protocol type: Este campo indica el tipo del protocolo original del paquete de los datos.
    - Checksum. Este campo contiene la suma de comprobación que se utiliza para ver si el paquete esta corrupto durante la transmisión. Esta información es opcional.

- Key: Esta información se utiliza para identificar o para autenticar la fuente real de los datos (iniciador).
- Sequence number: Este campo contiene un número que indica el número de secuencia del paquete en la serie que están siendo transmitidos.
- Source routing. Este campo contiene información adicional de enrutamiento. Este campo es opcional

- payload. El paquete original enviado por el iniciador al FA. También contiene el encabezado original.

10.1.6 . Tipos de túneles.

Los túneles pueden ser de dos tipos: voluntarios y obligatorios.

a. Túneles voluntarios.

Estos túneles son conocidos como end – to – end y son creados a petición de un usuario cliente. El nodo iniciador actúa como el túnel endpoint. Por lo tanto, un túnel separado se crea para cada par de comunicación. Después de que la comunicación entre los dos extremos se termina el túnel es terminado.

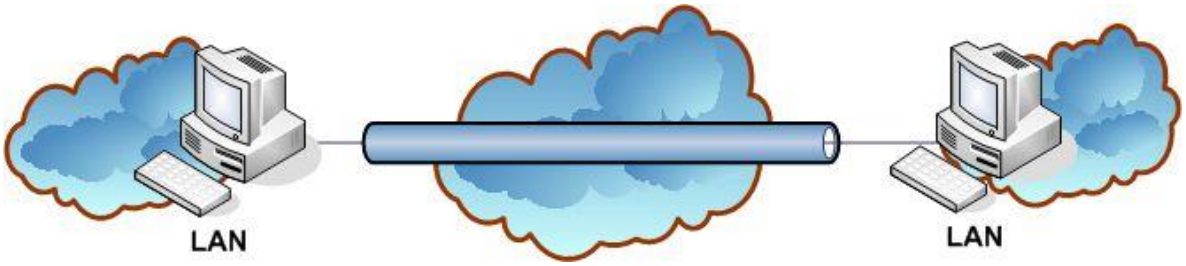


Figura 10.5 Túnel voluntario.

En el caso de un cliente remoto usando una conexión dial-up. El cliente primero necesita establecer una conexión dial-up en la red. Esto es un paso preliminar para establecer túneles lo cual no se logrado utilizando protocolos de túnel. Después de establecer una conexión dial-up puede el invitado fijar el túnel hasta el nodo destino previsto. Sin embargo, la situación es menos compleja en el caso de un cliente que

sea parte de la red local. En este caso, el cliente está conectado ya con la red interna. Por lo tanto, no necesita establecer una conexión separada dial-up para la red interna.

b. Túneles obligatorios.

A diferencia de los túneles voluntarios que son solicitados y creados por nodos del cliente, los túneles obligatorios son creados y configurados por un dispositivo intermedio. Tales dispositivos intermedios son: Network Attached Storages (NASs) o los servidores dial-up. Este tipo de túnel es obligatorio porque el iniciador debe utilizar el túnel creado por el dispositivo intermedio.

Nota: El dispositivo intermedio que se utiliza para instalar los túneles durante sesiones de VPN es conocido distintamente por diferentes protocolos de túneles por ejemplo: el L2TP se refiere a un dispositivo intermedio como un concentrador de acceso al L2TP, similarmente en terminología de PPTP el dispositivo se conoce como procesador de extremo delantero. En IPSec, el dispositivo intermedio que instala un túnel durante una sesión VPN se refiere comúnmente a la entrada de la seguridad IP.

En el caso de hacer un túnel obligatorio, ambos el cliente remoto como el cliente LAN debe conectarse con el dispositivo intermedio, que está situado generalmente en el ISP. Después de que la conexión se establezca con éxito, el dispositivo intermedio crea el túnel.

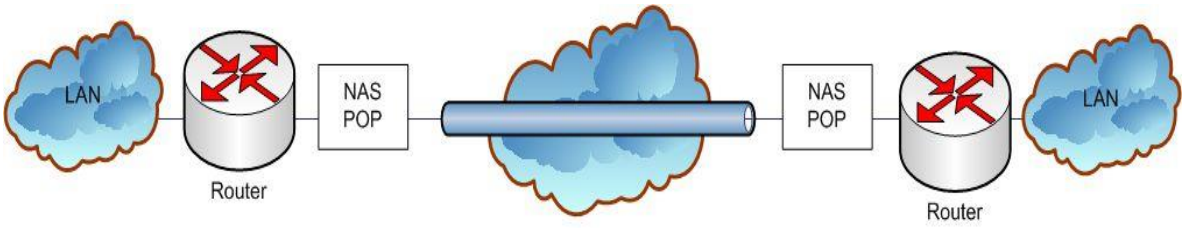


Figura 10.6 Túnel obligatorio.

Algunos expertos definen dos tipos de túneles basados en el período de actividad del túnel los cuales son: túneles estáticos y túneles dinámicos. Los túneles estáticos siguen siendo activos hasta que se termina, sin importar la transmisión de datos. Por consiguiente, estos tipos del túnel son costosos. Los túneles dinámicos de sitio-a-sitio VPNs. se activan solamente cuando los datos necesitan ser transferidos. Estos túneles son más seguros que los túneles estáticos.

10.1.7 Diferencia entre los dos tipos de túneles.

A continuación se describen algunas diferencias entre los dos tipos de túneles:

Túneles voluntarios	Túneles obligatorios
• El nodo del iniciador actúa como el punto final del túnel. • Un túnel separado se proporciona para cada comunicación en curso. • Se termina un túnel cuando el intercambio de datos entre los dos extremos esta completo. • El intercambio de datos entre los dos extremos es más rápido. • Éstos son túneles a corto plazo.	• El dispositivo intermedio actúa como el punto final del túnel. • El mismo túnel es compartido por múltiples comunicaciones en curso. • El túnel no es terminado hasta que el último par comunicándose complete la transacción de datos. • El intercambio de datos entre las dos entidades es lento porque el mismo túnel es compartido por múltiples comunicaciones. • Estos túneles son túneles a largo plazo.

Tabla 10.1 diferencia de los túneles.

10.1.8 Protocolos para crear túneles.

La tecnología para elaborar túneles hace uso de tres tipos de protocolos los cuales son.

Carrier Protocol: Estos protocolos se utilizan para encaminar los paquetes a través del túnel para llegar a su destino previsto a través de la red interna. Los paquetes de túnel se encapsulan dentro de los paquetes de este protocolo. Esto se debe a que los paquetes tienen que viajar a través de una red tal como es el Internet. Si los túneles se crean a través del Internet, el protocolo de transporte que comúnmente se utiliza es IP.

Encapsulating Protocol. Se utilizan estos protocolos para encapsular la carga útil. Además, el protocolo de encapsulado es también responsable de la creación, mantenimiento, y de la terminación del túnel. Hoy los protocolos más comúnmente usados para el encapsulamiento son: PPTP, L2TP, e IPSec.

Passenger Protocol. Los datos originales que necesitan ser encapsulados con el propósito de transmisión a través del túnel le pertenecen a este protocolo. Los protocolos que comúnmente son usados están: El PPP y el SLIP.

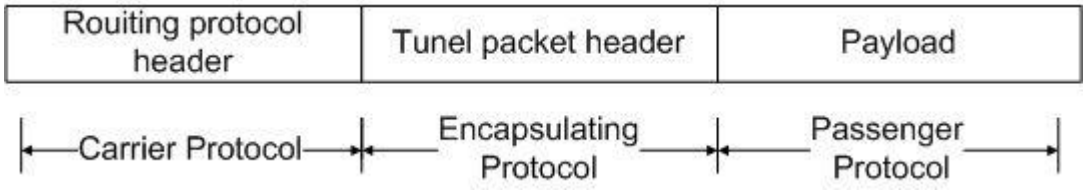


Figura 10.7 Formato del paquete del protocolo de túnel.

Los protocolos de túneles son fundamentales para asegurar y construir las sesiones a través de la VPN. Los protocolos comúnmente utilizados para crear túneles VPN funcionan en la capa de enlace de datos del modelo Open System Interconnect (OSI). A continuación se ilustra la capa en la que operan los protocolos que elaboran túneles:

Capas del modelo OSI	Protocolos para crear tuneles
Capa aplicación	No

Capa de presentación	No
Capa sesión	No
Capa transporte	No
Capa red	IPSec
Capa de enlace de datos	L2F, PPTP, L2TP
Capa física	No

Tabla 10.2 modelo OSI y protocolos para crear tuneles.

Los protocolos populares para crear un túnel que funciona en la capa 2 del modelo de OSI, según lo demostrado en el la tabla 1 son: Point-to-Point Tunneling Protocol (PPTP), Layer 2 Forwarding 2 (L2F), y Layer 2 Tunneling Protocol (L2TP). Además en la capa de red se encuentra IPSec. Antes de que estos protocolos se puedan discutir es esencial la comprensión del Point-to-Point Protocol (PPP).

10.2 PPP (POINT-TO-POINT PROTOCOL).

El PPP es un protocolo de encapsulación que facilita el transporte del tráfico de la red a través del enlace de datos point-to-point. La ventaja más grande del PPP es que puede funcionar en cualquier equipo terminal de datos (DTE) o en el equipo de la conexión de datos (DCE) incluyendo Eia/tia-232-c y de Itu-t V.35. Además un punto en favor del PPP es que no restringe la tasa de transmisión. Durante la transmisión, las únicas restricciones basadas en la transmisión son impuestas por la interfaz de DCE/DTE en uso. Finalmente, el único requisito del PPP es la disponibilidad de una conexión duplex (de dos vías), la cual puede ser síncrona o asincróna y un modo de operar cambiado o dedicado. El PPP es responsable de las siguientes funciones:

- Asignación y administración de direcciones IP y datagramas no-IP.
- La configuración y el análisis del enlace establecido.
- Encapsulación asíncrona y sincrona de datagramas.
- La detección de errores durante una transmisión.

- Multiplexación de múltiples protocolos de la capa de enlaces de datos.
- La negociación de parámetros de configuración es opcional, estos parámetros pueden ser la compresión de datos y direccionamiento.

El PPP realiza esta funcione con el uso de tres estándares:

- Estándar para encapsular los paquetes de los datos de un enlace Point-to-Point es: Link Control Protocol (LCP).
- Un estándar para establecer y configurar varios protocolos de la capa de red y detectar errores durante la transmisión es por medio del Network Control Protocol (NCP).

10.2.1 Operación del PPP.

Las operaciones del PPP son llevadas a cabo de la siguiente manera:

- Después de que los paquetes de datos se encapsulan, el nodo origen o iniciador envía frames LCP sobre el enlace point-to-point del nodo destino.
- Estos frames son usados para configurar el enlace de los parámetros específicos y controlar la estabilidad del enlace si se requiere.
- Después de que el nodo destino acepte la petición de conexión y su enlace este satisfactoriamente establecido se negocian las instalaciones opcionales. Estas son especificadas por LCPs
- El nodo origen envía frames NCP para elegir y configurar los protocolos de la capa de red.
- Después de que se configuran los protocolos requeridos de la capa de red, los dos extremos comienzan a intercambiar datos.

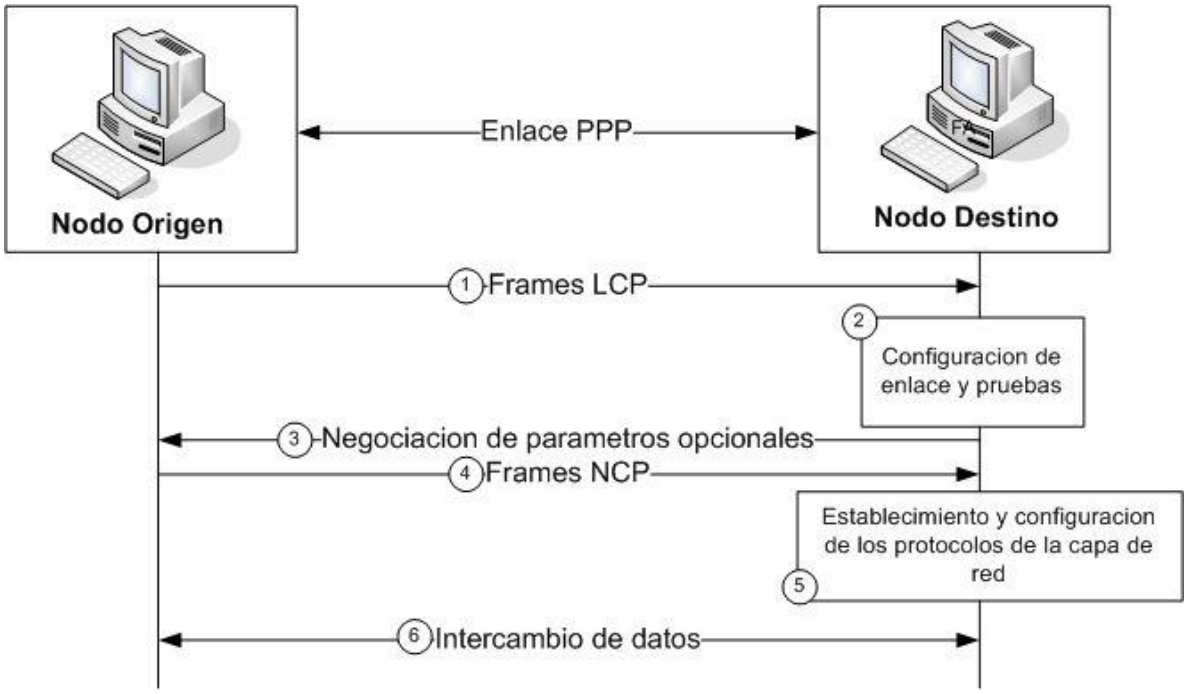


Figura 10.8 Estableciendo un enlace PPP y cambiando datos.

Cuando se establece un enlace PPP, existe hasta que los frames LCP o NCP señalan la terminación del enlace. El enlace también puede ser terminado en caso de un enlace fallido o la intervención de un usuario.

10.2.2 Formato del paquete PPP.

Seis campos constituyen un frame PPP. A continuación se describen cada uno de los siguientes campos:

- Flag: Este campo indica el inicio y el final de un frame. La longitud de este campo es de un byte.
- Address: PPP no utiliza las direcciones de nodos individuales. Por lo tanto, este campo contiene la secuencia binaria 11111111, que es una dirección de broadcast estándar. La longitud del campo es un byte.
- Control: Este campo contiene la secuencia binaria 00000011 , el cual denota que las frame llevan los datos del usuario. La longitud de este campo es un byte.

- Protocolo. Este campo identifica el protocolo de encapsulamiento. La longitud del campo es dos bytes. Sin embargo, esto es negociable a un byte si ambos pares coinciden.
- Datos. Este campo contiene la información existente cambiada entre el origen y los nodos de destino. La longitud de este campo varia, sin embargo la longitud máxima del campo puede estar en 1500 bytes.
- FCS (Frame Check Sequence).Este campo contiene la secuencia de cheque que ayuda al receptor a autenticar la exactitud de la información recibida en el campo de datos. Generalmente, la longitud de este campo es dos bytes. Sin embargo la implementación de PPP pueden negociar cuatro bytes con el propósito de mejorar y detectar los errores.

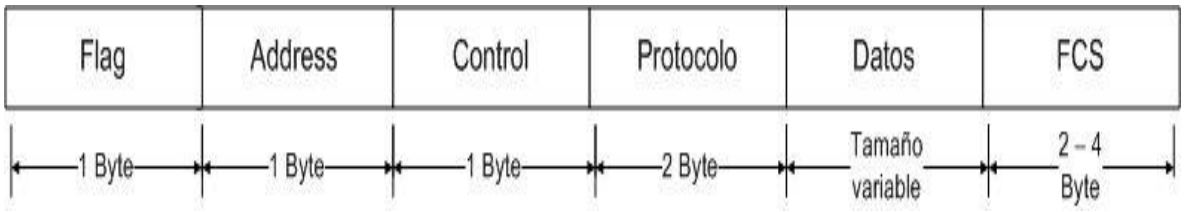


Figura 10.9 El formato de una frame PPP.

10.2.3 Enlace de control PPP.

Además del intercambio de datos exitoso entre dos nodos, el PPP es también responsable de controlar el enlace que se establece entre los dos extremos al comunicarse. El PPP utiliza LCP para este propósito, donde este es el responsable de las siguientes funciones:

- Ayuda a establecer el enlace PPP.
- Configurar el enlace establecido para satisfacerse los requisitos en la comunicación.
- Ejecutar mantenimientos regulares en el enlace PPP establecido.
- Terminar el enlace de los datos si el intercambio de datos entre los dos extremos esta completo.

Nota: en el caso de PPP, el termino enlace se refiere a la conexión point-to-point.
Link control protocol (LCP) ocurre en cuatro fases: la fase de establecer y negociar el enlace, la fase para determinar la calidad del enlace, la fase de negociación del protocolo de la capa de red, y la fase de la terminación del enlace. La descripción siguiente resume las cuatro fases del control del enlace.

- **La fase de establecer y negociar el enlace.** Antes de que cualquiera intercambio basado en PPP sea posible entre el origen y los nodos de destino, LCP debe establecer una conexión entre los dos extremos y negociar parámetros de la configuración. LCP utiliza los frames de enlace y establecimiento para este propósito. Cuando cada extremo responde con su propio frame ACK (acknowledgement), se termina esta fase.
- **Determinación de la calidad del enlace.** Esta es un fase opcional en la cual el enlace de calidad es establecido para determinar y verificar que el enlace esta listo para la negociar con el protocolo de la capa de red.

- **fase de negociación del protocolo de la capa de red.** En esta fase, lo fundamental es que se negocia el encapsulado de los datos en la estructura del campo del protocolo PPP.
- **Terminación del enlace.** Esta es la fase final de LCP y sirve para terminar el enlace establecido del PPP entre los dos extremos. La terminación del enlace puede ser agradecida o precipitada. La terminación agraciada del enlace ocurre después de que el intercambio de datos entre los dos extremos se ha completo o la petición de cualquiera de los extremos en terminar. La terminación precipitada ocurre cuando da lugar un acontecimiento físico tal como: la pérdida del portador o de la expiración de un contador de tiempo. Los frames de terminación del enlace se intercambian entre las partes involucradas antes que se desconecte el enlace.

La tecnología PPP es fundamental para otros protocolos de túneles usados hoy en día para crear VPN. En efecto todos los protocolos de túneles más populares se

basan en PPP y en la encapsulación de frames dentro de direcciones IP u otros datagramas para la transmisión a través de la red intermedia.

10.3 PPTP (POINT-TO-POINT TUNNELING PROTOCOL).

PPTP es una solución propietaria que permite la transferencia de datos de una manera segura entre un cliente remoto y un servidor de una organización. Esto lo realiza mediante, la creación de una VPN a través de la red interna basada en direcciones IP. Fue desarrollada por: Microsoft Corporation Ascend Communications, 3COM, US Robotics, and ECI Telematics. PPTP ofrece una garantía a las redes por medio de la creación de túneles, facilitando la transmisión de datos de una forma segura a través de la red pública y redes privadas.

Nota: Microsoft Corporation juega un papel clave en el desarrollo del PPTP, todos sus productos como por ejemplo: Windows NT (ediciones de servidor y puesto de trabajo) y Windows 2000, soporte naturalmente el PPTP.
Existen dos fenómenos que han jugado un papel importante en el éxito de las conexiones seguras PPTP. Éstos son:

- **El uso de PSTN (Public Switched Telephone Networks).** el PPTP permite el uso de PSTN para la ejecución de VPN. Como consecuencia, el proceso del despliegue de VPN es notablemente simple y los costos totales de la ejecución son significativamente pequeños. La razón de esto es simple, el costo. La necesidad de las corporaciones en soluciones que permitieran una conectividad por medio de líneas arrendadas y servidores de comunicación dedicados se elimina totalmente.
- **Soporte para los protocolos no IP**. Aunque esta basado para redes IP, PPTP soportan también otros protocolos de red tales como: TCP/IP, IPX, NetBEUI, and NetBIOS. Por esta razón PPTP ha demostrado ser tan efectivo en la creación de túneles ya sea para una red privada o una red pública.

10.3.1 El rol del ppp en las transacciones de PPTP.

PPP desempeña un papel importante en las transacciones basadas en PPTP debido a que es una extensión de PPP. PPTP no cambia la tecnología ya precedida por PPP, únicamente define una nueva manera de transportar tráfico PPP a través de redes públicas que no ofrecen ninguna garantía en seguridad. Las conexiones múltiples no son soportadas por ambos protocolos. Ya que Todas las conexiones PPTP deben ser Point-to-Point.

PPP satisface las funciones siguientes en las negociaciones basadas en PPTP:

- Establecer y terminar las conexiones físicas entre los extremos.
- Autenticar los clientes PPTP.

Encriptar IPX, NetBEUI, NetBIOS, y datagramas de TCP/IP para crear un datagramas PPP y asegurar los datos que se cambian entre las partes involucradas.

Nota: PPP puede usar texto limpio, encriptado o mecanismos de encriptación de Microsoft para autenticar al cliente PPP.

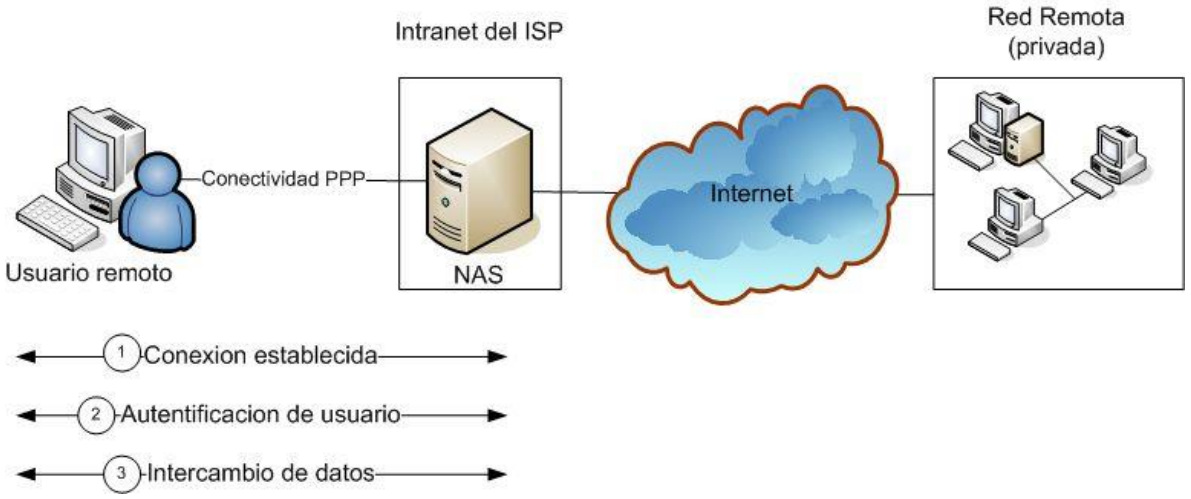


Figura 10.10 las tres responsabilidades del PPP en una transacción PPTP.

10.3.2 Los componentes de transacciones de PPTP.

Cualquier transacción basada en PPTP al menos contiene tres componentes los cuales son:

- Un cliente PPTP.
- Un Network Access Server (NAS).
- Un servidor PPTP.

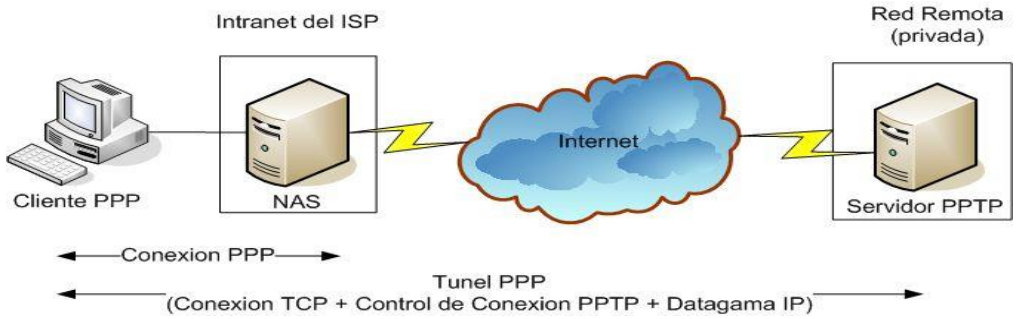


Figura 10.11 Un túnel PPTP y los tres componentes para las transacciones PPTP.

a. En cliente PPTP

Un cliente es un nodo de red que soporta PPTP y puede solicitar a otro nodo una sesión de VPN. Si la conexión es pedida por un servidor remoto, el cliente PPTP debe utilizar los servicios de un NAS y un ISP. Para esto, el cliente debe ser conectado con un módem, que se utiliza para establecer una conexión dial-up PPP con el ISP. Además se conectado con un dispositivo de VPN de modo que pueda hacer una petición a un dispositivo de una red remota para la creación del túnel. El enlace de la VPN remota utiliza la primera conexión dial-up conectada al ISP y al NAS para establecer un túnel entre los dispositivos de VPN a través del Internet o de otra red intermedia.

A diferencia de solicitudes remotas para las sesiones VPN, las solicitudes para una sesión VPN a un servidor local no requieren una conexión con el ISP y el NAS. Ambos el cliente y el servidor están físicamente unidos a la misma red LAN. El

cliente, en este caso, requiere solamente una sesión de dial-up establecida en la red con un dispositivo VPN.

La ruta de los paquetes PPTP para una petición remota y una petición local son diferentes, debido a que son asociados con peticiones de proceso distintas. Los paquetes de PPTP son colocados en servidor local unido al adaptador de la red del cliente de PPTP. Inversamente los paquetes PPTP de un servidor remoto son unidos por dispositivos físicos a un dispositivo de telecomunicación, tal como un router la colocación del los paquetes de la red se ilustra a continuación:

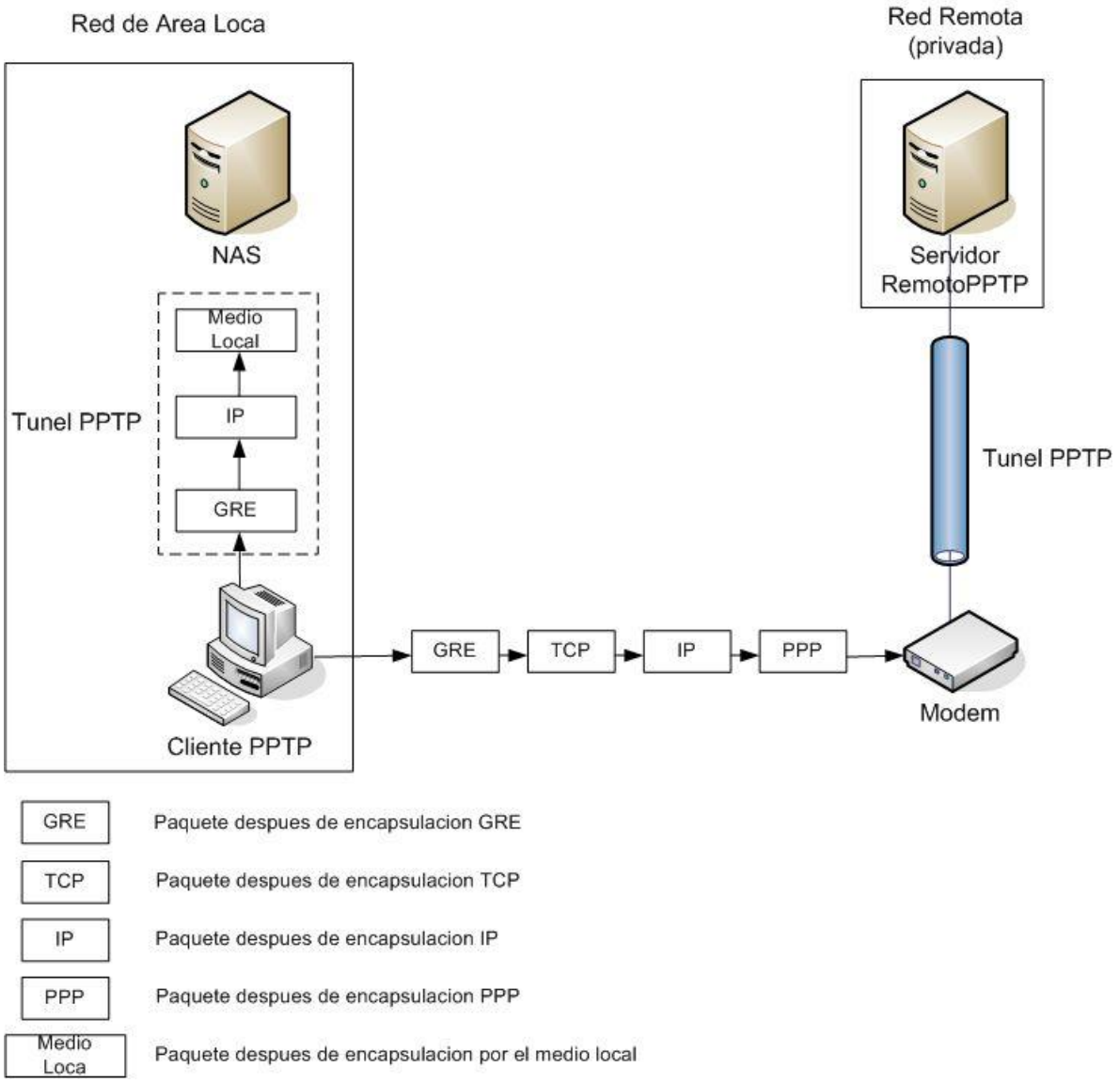


Figura 10.12 Transmitiendo paquetes PPTP a un nodo destino.

b. Servidor PPTP.

Los servidores PPTP son los nodos de red que soportan PPTP y son capaces de servir sesiones para VPN para nodos remotos o locales. Para responder a las peticiones remotas, estos servidores deben soportar las capacidades de asignación de rutas ya sea un servidor de acceso remoto o cualquier otro sistema operativo que soporte PPTP tal como: Windows NT o Windows 2000

c. PPTP Network Access Server (NAS).

Es establecido en el sitio del ISP y proporciona conectividad de Internet para clientes que usan PPP dial-in. Como la probabilidad de muchos clientes la petición de una sesión VPN simultáneamente es alta, estos servidores debe ser capaces de soportar múltiples clientes al mismo tiempo. Además los clientes no son solamente restringidos a Microsoft. Por lo tanto NAS debe manejar un amplio rango de clientes incluyendo los de Microsoft, Unix, Macintosh Apple entre otros. Sin embargo, es importante que estos clientes soporten conectividad PPTP con NAS.

10.3.3 Procesos del PPTP.

PPTP emplea tres procesos para asegurar la comunicación basadas en PPTP estos procesos son:

- establecimiento de conexiones basadas en PPP.
- control de la conexión.
- Tuénelo PPTP y transmisión de los datos.

a. Control de conexión PPTP.

Después de establecer las conexiones físicas basadas en PPP entre el cliente y el servidor PPTP, la conexión de control PPTP comienza a entrar. La conexión de control es establecida basada en direcciones IP del cliente y servidor PPTP. Además reserva el puerto TCP con el numero 1723.

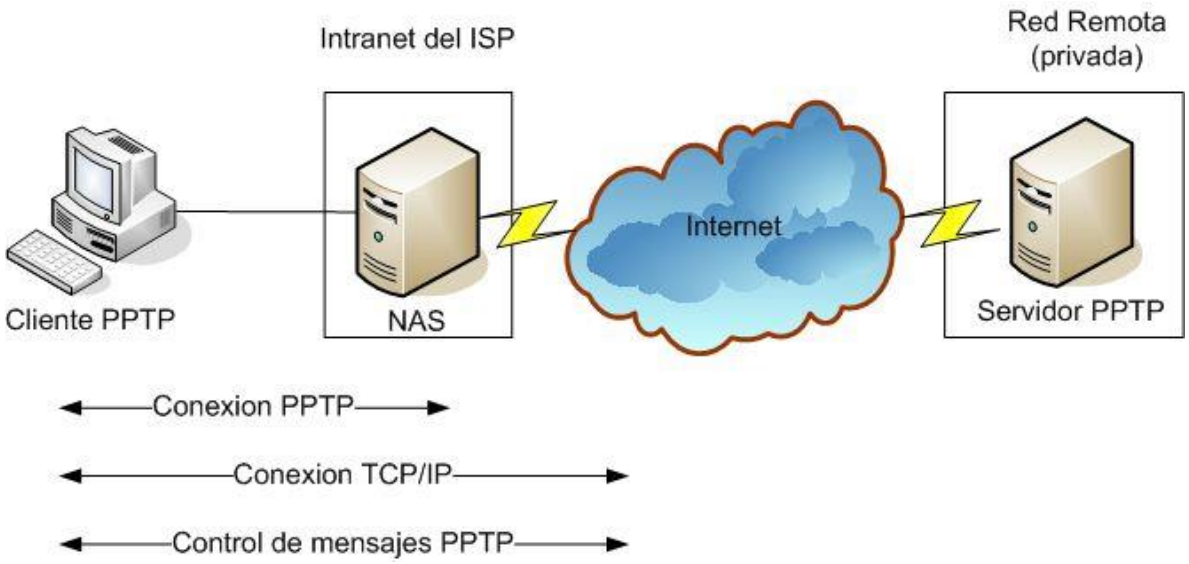


Figura 10.13 Cambiando mensajes de control PPTP a través de una conexión PPP.

El control de conexión es establecida para controlar y mantener por medio de mensajes que son cambiados entre las partes que se están comunicando. Los mensajes son los responsables de: mantener, administrar y terminar un túnel PPTP. Para mayor información visitar http://www.faqs.org/rfcs/rfc2637.html

Los mensajes de control son encapsulados en datagramas TCP Por lo tanto, después del establecimiento de una conexión PPP con el servidor o el cliente remoto, se establece una conexión TCP. Esta conexión se utiliza posteriormente para intercambiar mensajes de control PPTP.

b. Procesando datos a través del túnel PPTP.

Un paquete de los datos PPTP experimenta múltiples etapas de encapsulación las cuales son:

- La encapsulación de los datos. La información original (payload) es cifrada y luego encapsula dentro de un frame PPP. Un Header es adicionado al frame.
- La encapsulación de frame PPP. La frame resultante PPP es encapsula dentro de una encapsulación conocida como: Generic Routing Encapsulation

(GRE). La modificación del encabezado GRE contiene un campo Acknowledgement de cuatro byte y un bit que corresponde al Acknowledgement que notifica la presencia de un campo Acknowledgement. La llave del campo de la frame GRE se substituye por un campo de dos byte llamado Payload y otro campo de dos byte llamado Call ID. El cliente PPTP fija este campo cuando se crea el túnel PPTP.

- encapsulacion de paquetes GRE: El IP header se agrega la frame PPP, la cual es encapsula dentro del paquete GRE. Este IP header contiene las direcciones IP del cliente PPTP y del servidor destino

Encapsulación del dato en la capa de enlace: PPTP es un protocolo para construir tunes en la capa de enlace. Por lo tanto, el encabezado de dato en la capa de enlace juega un papel importante en la creación del túnel de datos. Antes de ser colocada en el medio de transmisión, la capa de trasmisión de datos agrega su propio encabezado y rastreador de datagrama. Si el datagrama tiene que viajar a través de un túnel local PPTP, el datagrama se encapsula con tecnología para LAN como por ejemplo: Ethernet. Por otra parte, si el túnel es referido a través de un enlace WAN, el encabezado y el rastreador que son agregados al datagrama son invariables una vez puestos en el PPP.

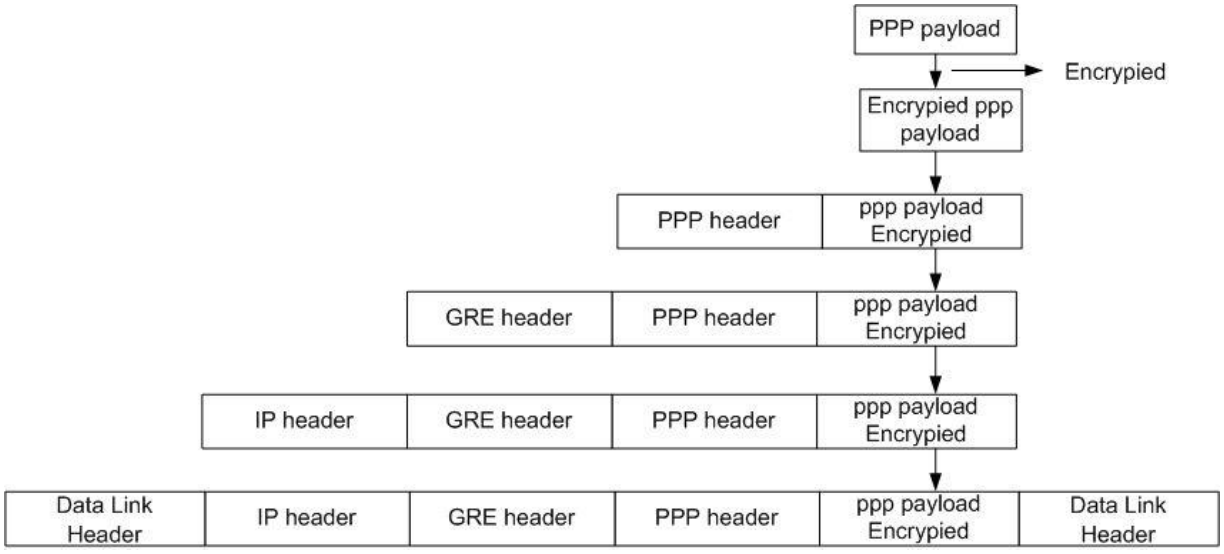


Figura 10.14 Proceso de los daros en PPTP.

GRE es un mecanismo simple, ligero y de uso general para la encapsulación de los datos basados en IP. GRE es utilizado generalmente por el ISPs para reenviar información de ruteo a las Intranet. Sin embargo, los router backbone de los ISP filtran este tráfico basado en GRE. Además, los túneles establecidos por PPTP pueden llevar los datos con seguridad y privacidad por medio de redes inseguras.

Cuando los datos PPTP se transfieren con éxito al receptor previsto, el receptor debe procesar los datos originales extrayéndolos del túnel. El proceso de extracción de datos basados en PPTP es exactamente al inverso de elabora un túnel de datos PPTP. Para recuperar los datos originales del nodo del cliente PPTP sigue los siguientes pasos:

- El extremo del receptor procesa y quita el encabezado de la capa de enlace que fueron agregados por el remitente.
- El encabezado GRE es quitado.
- El IP header es procesado y quitado.
- El PPP header es procesado y quitado.
- Finalmente, la información original es decodificada.

A continuación se describe el proceso para recuperar los datos por el receptor.

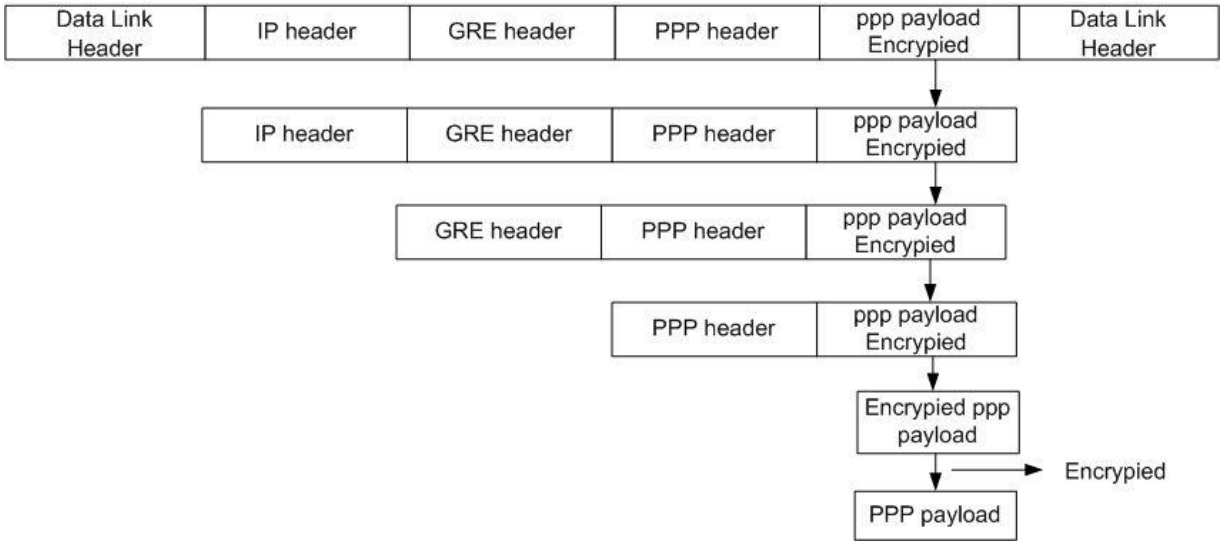


Figura 10.15 Procesando el dato el receptor.

10.3.4 Seguridad PPTP.

PPTP ofrece varios servicios de seguridad que están incorporados en los clientes y a los servidores PPTP. Estos servicios de seguridad incluyen lo siguiente:

- Codificación de datos y compresión.
- Autenticación.
- Control de acceso.
- Filtrado de paquete.

Además de los mecanismos de seguridad que anteriormente se mencionaron, PPTP se puede utilizar conjuntamente con cortafuegos y router.

a. **Codificación de datos y compresión.** PPTP no proporciona un mecanismo de codificación incorporado para asegurar datos. En vez, ello usa los servicios de codificación ofrecidos por PPP. PPP, a su vez, usa Microsoft Point-to-Point Encryption (MPPE), siendo este el método del cifrado.

   El secreto compartido usado para los propósitos de codificación en el caso del PPP es el ID de usuario y su contraseña correspondiente. La llave de la sesión es de 40-bit y es usada para cifrar la identificación del usuario y la contraseña mediante un algoritmo hashed que se almacena en el cliente y en el servidor.

   Hashed es el algoritmo que se utiliza para generar la llave RSA RC4. Esta llave permite cifrar todos los datos que se transfieren a través del túnel. Sin embargo, una llave 40-bit es demasiado corta y demasiado débil para las técnicas avanzadas de hacking de hoy en día. Debido a esto, esta disponible una nueva versión de 128-bit que disminuye los riesgo de seguridad. Microsoft recomienda que la llave se deba renovar después de cada 256 paquetes.

b. **Autenticación PPTP.** PPTP soporta los siguientes mecanismos de autentificación:

- MS-CHAP (Microsoft Challenge Handshake Authentication Protocol). MS-CHAP es una versión modificada de CHAP realizada por Microsoft, además es utilizada para las autentificaciones basadas en PPP. Debido a su fuerte afinidad a CHAP, la funcionalidad de Ms-CHAP es absolutamente similar a la de la CHAP. La diferencia principal entre el dos es que CHAP esta basada en el algoritmo hash RSA MD5, mientras que MS-CHAP esta basada en RSA RC4 y DES. Ms-CHAP fue desarrollado solamente para los productos de Microsoft (Windows 9x y varias versiones de Windows NT), MS CHAP no es soportado por otras plataformas.
- **PAP (Password Authentication Protocol).** El PAP es el más simple y el mas comúnmente implementado en la autenticacion dial-in. También se utiliza para autenticar conexiones basadas en PPP. Sin embargo, envía la identificación del usuario y la contraseña en un formato no encriptado a través del enlace. Por lo tanto, no ofrece ninguna protección contra las los ataques. Otra dificultad del PAP es que los extremos al comunicarse están autenticados solamente una vez en el establecimiento de la conexión. Si un craker asume con éxito el control de la conexión, él o ella no tendría preocupaciones acerca de la autentificación adicional. Debido a estas razones, el PAP se considera el protocolo menos sofisticado para la autentificación y no es el mecanismo preferido para la autentificación en las VPNs.

c. **Control de acceso de PPTP.** Después de que autentique a un cliente remoto PPTP, su acceso a los recursos dentro de la red puden ser restringidos con el fin de obtener una mayor seguridad. Este objetivo es alcanzado por la puesta en práctica de los mecanismos de control de acceso, tales como:

- Derechos de acceso
- Permisos
- Workgroups

d. **Filtrado de paquete PPTP.** La filtración de paquetes PPTP permite que un servidor PPTP en una red privada acepte y enrute los paquetes solamente de esos clientes PPTP que se han autenticado con éxito. Consecuentemente, solamente los clientes autorizados por PPTP pueden acceder a la red remota específica. De este modo, PPTP proporciona no sólo la autentificación, el control de acceso, y mecanismos del cifrado, sino que también aumenta la seguridad de la red.

10.3.5 PPTP con firewalls y router.

Cuando PPTP es utilizado conjuntamente con los router y los firewalls, el tráfico destinado para estos puertos se encamina a través del cortafuego o del router, ya que filtran el tráfico en base de las listas del control de acceso (ACLs) y otras estrategias de la seguridad. De esta manera, PPTP fomenta los servicios de seguridad.

10.3.6 Las ventajas y desventajas del PPTP

Las ventajas principales ofrecidas por PPTP son las siguientes:

- PPTP es una solución incorporada con los productos Microsoft, los cuales son ampliamente usados.
- PPTP puede soportar los protocolos basados en no IP.
- PPTP es soportado por varias plataformas, tal como UNIX, Microsoft y Apple Macintosh. Otras plataformas que no apoyan PPTP pueden ayudar con los servicios PPTP usando un router para que realice las funciones de un cliente PPTP.

La implementación de PPTP tiene ciertas desventajas las cuales son:

- PPTP es una opción débil comparada con L2TP e IPSec que son tecnologías mucho más seguras.
- PPTP es una plataforma dependiente.
- PPTP requiere configuración extensiva tanto en el servidor como en el cliente PPTP.
- La inseguridad del protocolo PPTP. El popular criptólogo Bruce Schneier (fundador de la consultora norteamericana Counterpane Systems) ha descubierto numerosos problemas de seguridad en las implementaciones PPTP de Microsoft. Y dice "aunque se han corregido muchos de los problemas denunciados en la implementación previa, algunos de ellos siguen presentes. Peor aún, algunos de los cambios realizados debilitan considerablemente la calidad del sistema".

- PPTP es un protocolo que puede evitar al curioso casual, pero no es rival ante un adversario determinado a acceder a la información que circule por el túnel. Este hecho es especialmente importante para las corporaciones que emplean PPTP para interconectar sus intranets entre sí, a través de infraestructuras públicas como es Internet.

Ahora L2TP, el sustituto del PPTP, es ya una propuesta oficial de estándar, tras varios años de desarrollo, la única excusa para seguir usando PPTP es el hecho de que este software viene incluido con los sistemas operativos Windows. Pero cualquier administrador que pueda elegir debe implementar L2TP. L2TP, al contrario que PPTP, ha sido desarrollado por multitud de empresas y especialistas en el campo de las VPN, y es un estándar abierto no atado a ninguna arquitectura en particular.

10.4 L2F (LAYER 2 FORWARDING).

Los servicios de redes dial-up fueron realizados a través del Internet y posteriormente fueron sobre la tecnología IP. Esta es la razón por la cual las soluciones populares para crear túneles, tales como: PPP y PPTP, demostraron ser

más exitosas con la infraestructura IP que otras tecnologías contemporáneas, tales como: ATM y Frame Relay, entre otras.

A pesar de los reclamos de Microsoft para asegurar las transacciones, PPTP fue basado en Ms-CHAP, que, como se dijo en la sección anterior, no es muy seguro. Estos asuntos hicieron que las organizaciones y los expertos de la industria buscaran soluciones alternativas que ofrecieran servicios dial-up y soporte para múltiples protocolos que se podrían ocupar para la creación de túneles.

Cisco Systems, junto con Nortel, eran uno de los vendedores principales que comenzaron a trabajar hacia una solución que: Habilitara transacciones seguras, proporcionara acceso a la infraestructura subyacente del Internet y a otras redes públicas sirviendo como un puente intermedio y por ultimo que soporte una amplia gama de tecnologías de red, tal como ATM, FDDI, IPX, Net-BEUI, y Frame Relay.

La alternativa que Cisco presentó después de una investigación extensa fue L2F. L2F ofreció otro adelanto importante en tecnología de acceso remoto, porque soportar más de una sesión simultanea dentro del mismo túnel. En términos más simples, más de un usuario remoto puede acceder a una Intranet privada usando una conexión sencilla dial-up. L2F alcanzó esto definiendo conexiones múltiples dentro de un túnel donde cada conexión representa una sola cadena PPP.

Esta cadena puede originarse de un solo usuario remoto o de usuarios múltiples. Debido a que el túnel puede soportar conexiones múltiples simultáneamente, menos conexiones se requieren de un sitio remoto ISP y del ISP POP del gateway de una red privada. Esta característica es especialmente útil en la reducción de costos.

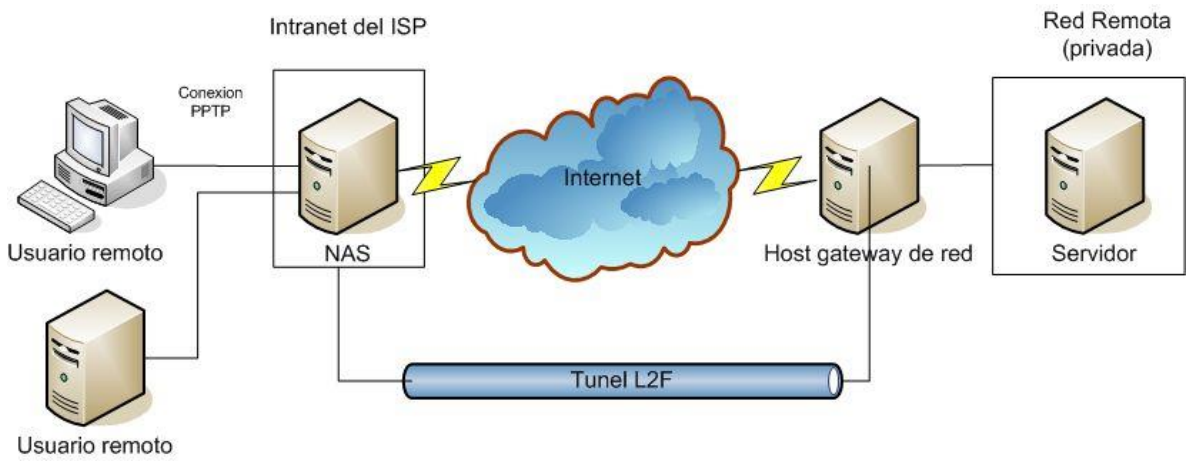


Figura 10.16 Tunel L2F desde un ISP's POP a un gateway de una red privada

10.4.1 Los procesos del L2F.

Cuando un cliente remoto inicia una conexión dial-up a un host situado en un Intranet privada, los procesos siguientes son ejecutados de una manera secuencial:

- Los usuarios remotos inician una conexión PPP con su ISP. Si el usuario remoto es parte de una LAN el usuario puede emplear el ISND u otra conexión alternativa con el ISP. si el usuario no es parte de ninguna Intranet, él o ella necesitará utilizar los servicios fundamentales de un PSTN.
- Si NAS presente con el ISP POP acepta la petición de conexión, la conexión del PPP se establece entre la NAS y el usuario.
- Los usuarios en los extremos del ISP son autenticados con CHAP o PAP
- Si ningún túnel existe el gateway destinado o deseado de la red es iniciado.
- Después de que el túnel se establezca con éxito, una identificación única del múltiplex ID (MID) es asigna a la conexión. también se envía un mensaje de notificación al gateway de la red. Este mensaje notifica al gateway sobre el pedido la conexión de un usuario remoto.
- La gateway puede aceptar la petición de conexión o rechazarla. Si se rechaza la petición, notifican al usuario sobre la falta de la petición y se termina la conexión dial-up. Por otra parte, si se acepta la petición, el gateway envía la notificación de inicio al cliente remoto. Esta respuesta puede también incluir la

información de la autentificación, que es utilizada por el gateway para autenticar al usuario remoto.

Después que el usuario es autenticado por el gateway de la red una interfaz virtual se establece entre los dos extremos.

Nota: Si CHAP se utiliza para la autentificación del usuario, según lo especificado en el paso 6, la respuesta incluye el reto del username, y la respuesta cruda. Para las autentificaciones basadas en PAP, la respuesta incluye el username y contraseña en claro texto. En el caso del PPP, la notificación inicial también incluye los mensajes de CONFACK que se intercambian entre los dos extremos, después de una negociación acertada del TCP. Estos reconocimientos permiten al gateway de la red que inicialice su propio estado PPP, eliminando la necesidad de negociación de una fase adicional de LCP.

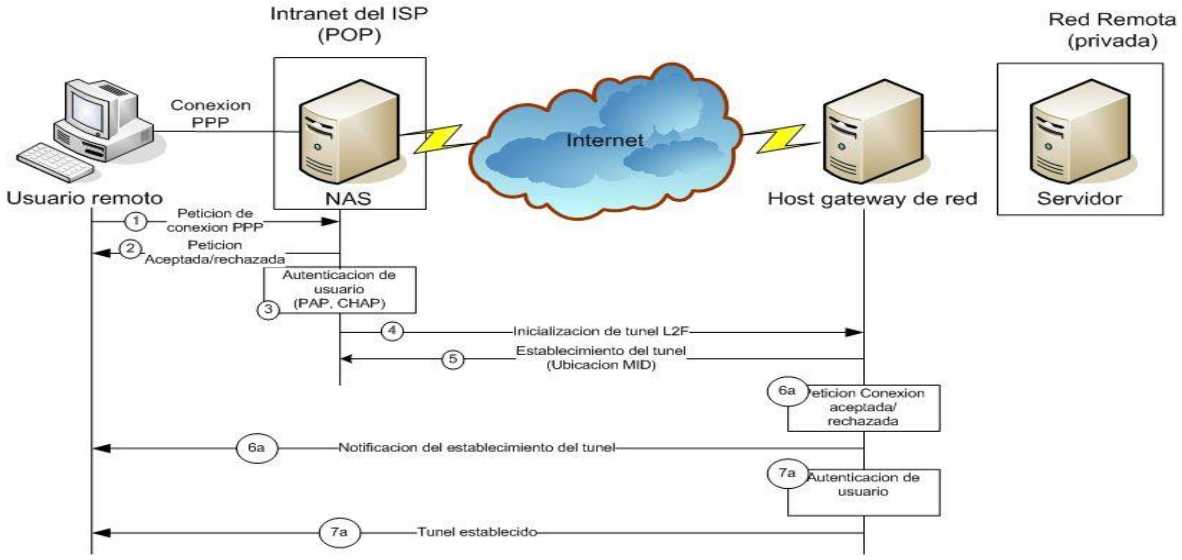


Figura 10.17 Estableciendo un túnel L2F entre un usuario remoto y un servidor.

10.4.2 El túnel L2F.

Cuando un usuario remoto es autenticado y acepta la petición de conexión, un túnel se establece entre el NAS del ISP y el host remoto de la red. Después de realizar un túnel entre los dos extremos la capa de enlace puede intercambiar frames sobre el túnel de la siguiente manera:

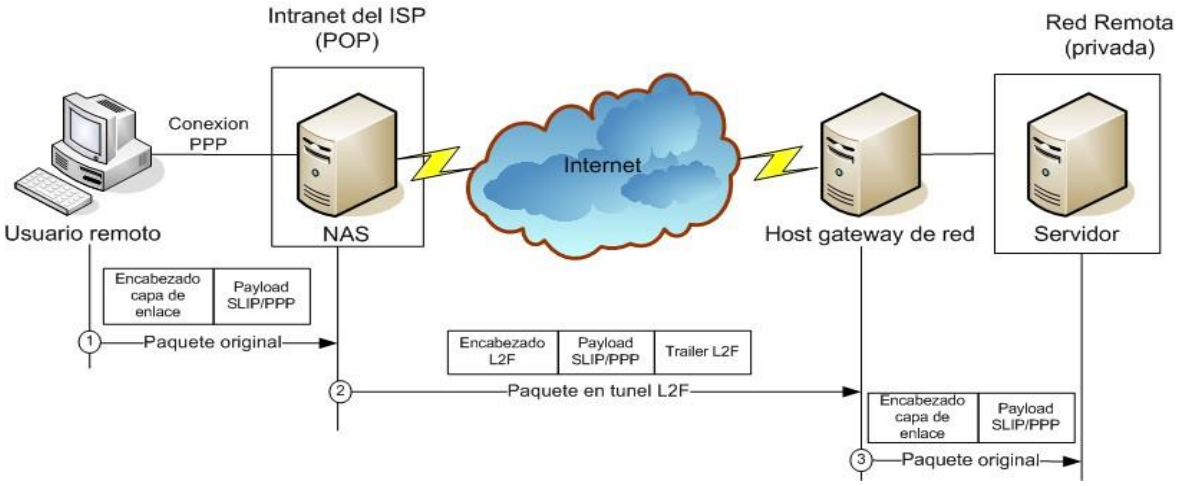


Figura 10.18 Proceso del tuneleo L2F

- El usuario remoto transmite frames normales al NAS localizado en el ISP.
- POP quita la información de la capa de enlace y la adiciona al encabezado L2F. El encapsulado reciente de la frame es enviada a la red destino por medio del túnel.
- El gateway de red acepta éstos paquetes que han viajado en el tunel, extrae el encabezado del L2F y transmite las frames al nodo destino dentro de la Intranet.
- El nodo destino procesa los frames recibidas como non-tunneled fremes.

Nota: Los túneles L2F también se conocen como "interfaces virtuales"

Cualquier respuesta del host destino experimenta el proceso inverso. Es decir, el host envía un frame normal a la capa de enlaces de datos del getaway, la frame es capsula en un paquete L2F (demostrado en el cuadro 5-14), y la transmite al NAS situado en el sitio del ISP. el NAS extrae la información de la frame L2F y agrega la información apropiada de la capa de enlace de datos. La frame se remite al usuario remoto.

L2F Header	Payload Paquet (PPP/SLIP)	L2F Checksum

Figura 10.19 forma del paquete L2F

10.4.3 Seguridad L2F

L2F proporciona los siguientes servicios:

- Data encryption
- Authentication

a. **L2F Data Encryption:** L2F utiliza MPPE (Microsoft Point-to-Point Encryption) para los propósitos básicos del cifrado. Sin embargo, MPPE no es una técnica segura contra las técnicas de hacking que existen hoy en dia. por esta razon el L2F utiliza también el cifrado basado en Internet Protocol Security (IPSec) para asegurarse de que los datos estén seguros durante transmisiones. IPSec utiliza dos protocolos para los propósitos del cifrado Encapsulating Security Payload (ESP) y Authentication Header (AH). Además para asegurar el intercambio de llaves durante la fase key-exchange, IPSec también usa el protocolo llamado: Internet Key Exchange (IKE).

   La ventaja más grande de la tecnología basada en el cifrado IPSec es que fuerza la autentificación de cada paquete individualmente en vez de la práctica común de la autentificación del usuario. los mecanismos de autentificación de cada usuario, comunicándose en los extremos es autenticado solamente una vez al principio de la comunicación. Sin embargo, la estrategia de la autentificación de paquetes es más lenta que la estrategia de la autentificación de usuarios. IPSec se ha recomendado como el protocolo mas seguro para todos los túneles de VPN.

b. **L2F Authentication:** La autentificación del L2F se logra en dos niveles. El primer nivel de la autentificación basada en L2F ocurre cuando el usuario remoto marca hacia el punto de presencia (POP) del ISP. Aquí en delante los procesos de establecimiento del túnel comienza solamente después que han

autenticado al usuario. El segundo nivel de la autentificación es hecho por el gateway de la red, no establece un túnel entre los dos extremos hasta que autentica al usuario remoto.

L2F utiliza también los servicios de seguridad soportados por PPP para los propósitos de la autentificación. Además el PAP para autenticar a un cliente remoto cuando una gateway L2F recibe una petición de conexión. L2F utiliza los siguientes protocolos de autentificación para la seguridad de datos:

- **CHAP (Challenge Handshake Authentication Protocol):** CHAP fue desarrollado para tratar el problema de enviar contraseñas en texto limpio mientras se usaba el PAP. En CHAP, cuando el cliente es cuestionado por su identificación, responde con un valor secreto de HASH derivado del algoritmo de cálculo MD5. si valor hash es calculado por el servidor usando procedimiento enviado por el cliente. Este es autenticado exitosamente. Por lo tanto no se intercambia ninguna contraseña en texto limpio durante el proceso. Un problema asociado comúnmente al PAP es que la comunicación entre los extremos es autenticada solamente una vez durante el proceso entero de la comunicación. el CHAP, sin embargo, puede forzar múltiples autentificación durante una sesión, el cual dificulta que un hacker fuerce la entrada de comunicación.

- **EAP (Extensible Authentication Protocol):** A diferencia de los métodos PAP y CHAP los cuales son ejecutados a la hora de la configuración de LCP, durante la disposición de la conexión PPP. El EAP es ejecutado después de la fase del LCP, cuando la autentificación PPP es realizada. Por lo tanto, EAP permite la autentificación extensa debido al número creciente de parámetros de conexión que se puede utilizar opcionalmente como información de la autentificación.

Nota: el L2F también utiliza Shiva Password Authentication Protocol (SPAP) para la autenticación. SPAP es un protocolo propietario que usa contraseñas encriptadas y puede soportar características mejoradas tales como: cambios de contraseñas y soporte para mecanismos de rellamada.

Además de los mecanismos ya mencionados de autentificación, L2F emplea Remote Access Dial-In User Service (RADIUS) y Terminal Access Controller Access Control Service (TACACS) como servicios adicionales para la autenticación. Ambos servicios autentican a usuarios que acceden al servidor local de acceso remoto. RADIUS y TACACS es generalmente implementado por el ISP y en gran escala en corporaciones.

Nota: RAS es generalmente capaz de procesar una petición de conexión remota y de conceder el acceso. Sin embargo, si el número de usuarios remotos es muy grande, puede enviar la petición a un servidor RADIUS, TACACS o a una base de datos conectada que puedan autenticar al usuario y conceder o negar el acceso.

10.4.4 Ventajas y desventajas del L2F.

Auque L2F requieren extensiones que negocian con diferentes opciones de LCP y opciones de autenticación es mas extenso que PPTP debido ha que es una solución que envía frame a bajo nivel. También proporciona una mejor plataforma en soluciones de VPN para las redes de las corporaciones que PPTP.
Las ventajas principales para implementar soluciones basadas en L2F son las siguientes:

- Incremento de la seguridad en las transacciones.
- Plataforma independiente
- No necesita acomodamientos especiales con el ISP
- Soporta un rango amplio de tecnologías de red tales como: ATM, FDDI, IPX, NetBEUI, y Frame Relay

A pesar de las ventajas mencionadas, hay algunas desventajas asociadas a L2F las cuales son:

- Las soluciones basadas en L2F requieren una extensiva configuración y un soporte continuo.
- La implementación de una solución basada en L2F es altamente dependiente del ISP. Si el ISP no soporta L2F, la implementación de la solución no es posible.
- L2F no proporciona control de flujo. Como resultado si el túnel es llenado con paquetes de datos puede caerse arbitrariamente. Esto causa la retransmisión de los datos, que alternadamente retardan la velocidad de la transacción.
- Las transacciones realizadas a través de los túneles basadas en L2F es lento cuando se compara con PPTP.

Nota: para mayor información sobre L2F referirse a la siguiente dirección http://www.armware.dk/RFC/rfc/rfc2341.html.

Con el desarrollo de L2F, había dos tecnologías para crear un túnel, PPTP y L2F. Estas dos tecnologías competían para el control del mercado siendo los dos protocolos incompatibles. Por esta razón, las corporaciones son cuidadosas porque cada una tiene diferentes requerimientos. El IETF decidió terminar la confusión y asignar por mandato que las características de las dos tecnologías estuvieran combinadas para producir un protocolo que sería utilizado como estándar en soluciones de VPN. El protocolo resultante del mandato para crear un túnel en la capa de enlace de datos fue el: L2TP.

10.5. L2TP (LAYER 2 TUNNELING PROTOCOL).

Desarrollado por IETF y respaldado por gigantes de la industria, tales como Cisco Systems, Microsoft, 3COM and Ascend, L2TP es una combinación de PPTP y L2F. De hecho fusiona las mejores características de PPTP y L2F. L2PT provee la

flexibilidad, escalabilidad y el buen precio de la solución de acceso remoto de L2F y la rápida conexión punto a punto de PPTP.

Los beneficios claves que ofrece L2TP, son una mezcla de los atributos de PPTP y L2F. A continuación se presenta una lista de estos beneficios:

- L2TP soporta múltiples protocolos y tecnologías de red, tales como IP, ATM, Frame Relay y PPP. Como resultado puede soportar diversas tecnologías con una infraestructura de acceso común.
- L2TP permite a varias tecnologías dar un empuje a las infraestructuras de acceso intermedio de la Internet y otras redes públicas, tales como PSTNs.
- L2TP no requiere implementación de software adicional, tal como drivers adicionales o soporte de sistema operativo. Consecuentemente ni el usuario remoto ni la intranet privada necesita implementar software especial.
- L2TP permite a usuarios remotos con direcciones IP no registradas o privadas acceder una red remota a través de una red pública.
- La autenticación y autorización L2TP es realizada por el gateway de la red. Por lo tanto los ISPs no necesitan mantener una base de datos de autorizaciones o de derechos de acceso para usuarios remotos. Además las intranets privadas pueden también definir sus propias políticas de acceso y seguridad. Esto hace el proceso de establecimiento de túneles mucho más rápido que con los protocolos antes mencionados.

La característica principal de los túneles L2PT es que establecen túneles PPP que a diferencia de los PPTP, no se terminan a en el sitio ISP más cercano, en su lugar, estos túneles se extienden al gateway de la red. Las solicitudes para túneles L2TP pueden ser iniciadas por el usuario remoto o por gateway del ISP.

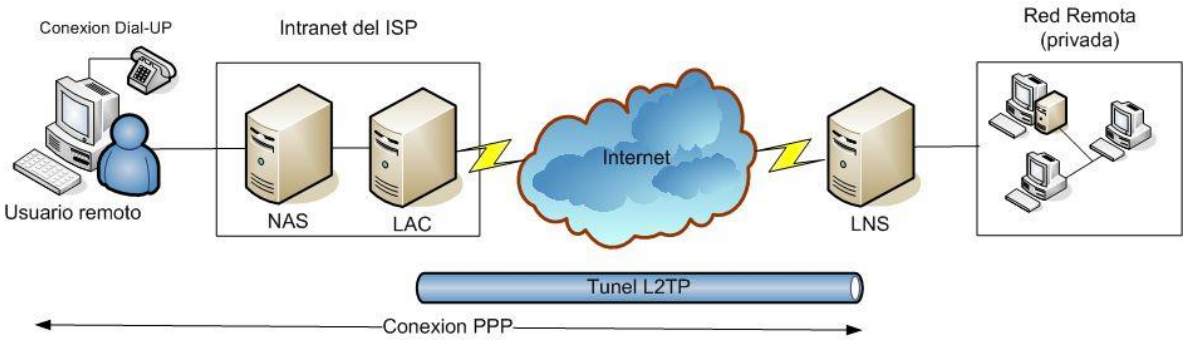


Figura 10.20 El tunel L2TP

Cuando las tramas PPP son enviadas a través del túnel L2TP, son encapsuladas como mensajes UDP. L2TP utiliza mensajes UDP para enviar los datos a través del túnel y para paquetes de mantenimiento del túnel, a diferencia de los protocolos anteriores, este tiene la misma estructura de paquetes.

10.5.1 Componentes del L2TP.

Las transacciones basadas en L2TP básicamente emplean tres componentes, un Network Access Server (NAS), un L2TP Access Concentrator (LAC), y un *Network Server* L2TP (*LNS*).

a. **Network Access Server (NAS):** Los NAS L2TP son dispositivos de acceso punto a punto que proveen conectividad al Internet en base a la demanda de un usuario remoto que realiza conexiones PPP. Los NAS son responsables de la autenticación de los usuarios remotos al nivel del ISP y determinar si una conexión dial up virtual es requerida. Como en los NAS PPTP, los NAS L2TP están localizados en el sitio ISP y actúan como cliente en el proceso de establecimiento de túneles. Los servidores NAS pueden responder a múltiples solicitudes de conexión y pueden dar soporte a un amplio rango de clientes como por ejemplo: Microsoft, Unix, Linux, VAX-VMS entre otros.

b. **L2TP Access Concentrator (LAC):** El papel de los LACs en la tecnología de túneles L2TP es establecer un túnel a través de una red pública tal como:

PSTN, ISDN o el Internet hacia el LNS en la red anfitriona. De esta manera, los LACs sirven como punto de terminación del medio físico entre el equipo del cliente y los LNS de la red anfitriona.

Nota: El punto más importante a recordar acerca de los LACs es que ellos están generalmente localizados en el sitio del ISP.

c. **Network Server L2TP (LNS):** Los servidores de red L2TP, como se mencionó anteriormente, se encuentran localizados en el lado de la red anfitriona. Por lo tanto son utilizados para terminar la conexión L2TP en el lado de la red anfitriona en la misma manera en que los LACs terminan el túnel del lado del cliente. Cuando un LNS recibe una solicitud para una conexión virtual desde un LAC, se establece el túnel y autentica al usuario quien realizó la solicitud de conexión. Si el LNS acepta la solicitud de conexión, crea la interfase virtual.

10.5.2 Procesos L2TP.

Cuando un usuario remoto necesita establecer un túnel L2TP a través del Internet u otra red pública, ocurre la siguiente secuencia de pasos.

- El usuario remoto envía una solicitud de conexión al NAS del ISP más cercano y haciendo esto inicia una conexión PPP con el lado del ISP.
- El NAS acepta la solicitud de conexión luego de autenticar al usuario final. NAS utiliza métodos de autenticación PPP tales como PAP, CHAP, SPAP y EAP.
- El NAS activa el LAC, el cual obtiene del LNS la información de la red destino.
- A continuación el LAC establece un túnel LAC-LNS sobre la red intermedia entre los dos puntos. El medio del túnel puede ser también ATM, Frame Relay o IP/UDP.

- El túnel es establecido satisfactoriamente. LAC asigna un identificador de llamada Call ID (CID) a la conexión y envía un mensaje de notificación al LNS. Este mensaje de notificación contiene información que puede ser utilizada para autenticar al usuario remoto. El mensaje también lleva opciones LCP que han sido negociadas entre el usuario y el LAC.
- El LNS utiliza la información recibida dentro del mensaje de notificación para autenticar al usuario. Si el usuario es autenticado de manera satisfactoria y el LNS acepta la solicitud de túnel, una interfase virtual PPP (túnel L2TP) es establecida con la ayuda de las opciones LCP recibidas en el mensaje de notificación.
- El usuario remoto y el LNS comienzan a intercambiar datos a través del túnel.

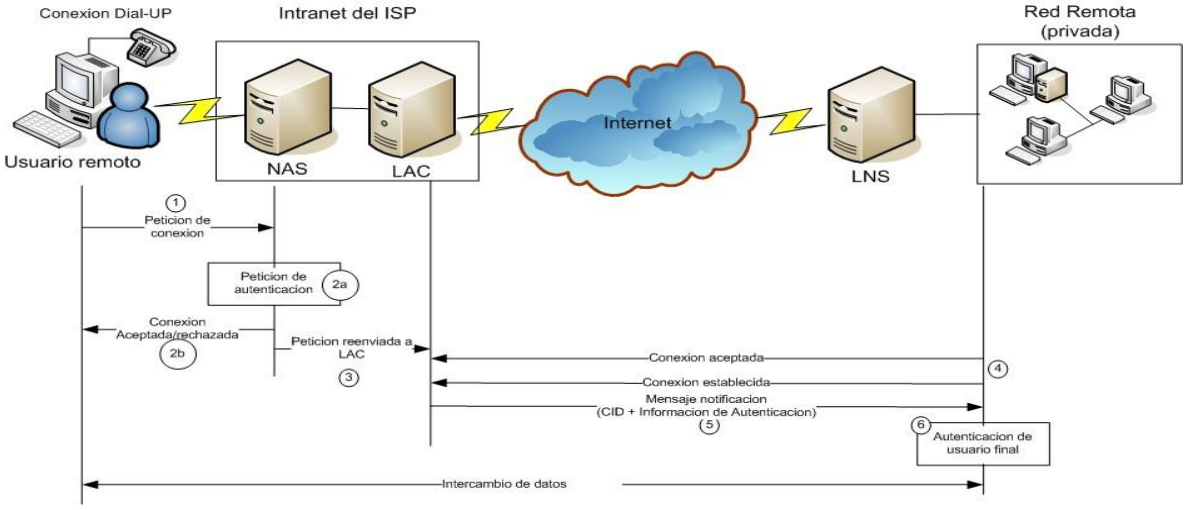


Figura 10.21 Estableciendo un túnel L2TF.

L2TP como PPTP y L2F soporta dos modos de operación, los cuales son:

a. **Modo de llamada entrante:** En este modo de operación la solicitud de conexión es iniciada por el usuario remoto.

b. **Modo de llamada saliente:** En este modo de operación, la solicitud de conexión es iniciada pro el LNS. Por lo tanto el LNS le indica al LAC realizar una llamada al usuario remoto. Luego de que el LAC establece la llamada el usuario remoto y el LNS pueden intercambiar paquetes a través del túnel.

10.5.3 Envío de datos a través de túneles L2TP.

Similar a los paquetes enviados por túneles PPTP, los paquetes de datos L2TP pasan por múltiples niveles de encapsulado. Los cuales se describen a continuación:

- **Encapsulado de datos PPP.** A diferencia del encapsulado PPTP, los datos no se encriptan previamente. Solamente se agrega una cabecera PPP a los datos originales.
- **Encapsulado de datos L2TP:** Luego de agregar la cabecera PPP se agrega una cabecera L2TP.
- Encapsulado UDP de las tramas L2TP: La trama L2TP se encapsula en una trama UDP. Los puertos de origen y destino dentro de la cabecera UDP son seteados a 1701 de acuerdo a las especificaciones L2TP
- **Encapsulado IPSec de datagramas UDP**: Luego de que la trama L2TP es encapsulada en UDP, esta trama UDP es encriptada y una cabecera IPSec ESP es agregada.

El proceso de obtener los datos del túnel L2TP es inverso al de poner los datos en el túnel L2TP.

10.5.4. Modos de túneles L2TP

L2TP soporta dos modos de túneles, el modo de túnel obligatorio y el modo de túnel voluntario. Estos túneles juegan un papel importante en la transmisión segura de datos de un destino a otro.

a. **Modo de túnel L2TP obligatorio:** Un túnel L2TP obligatorio se establece entre el LAC en el lado del ISP y el LNS en la red anfitriona. Es importante para el establecimiento exitoso de un túnel obligatorio que el ISP soporte la tecnología L2TP. Además, el ISP juega un papel clave en el establecimiento

de túneles L2TP porque es en el lado del ISP que se decide cuando es requerido un túnel obligatorio para una sesión determinada.

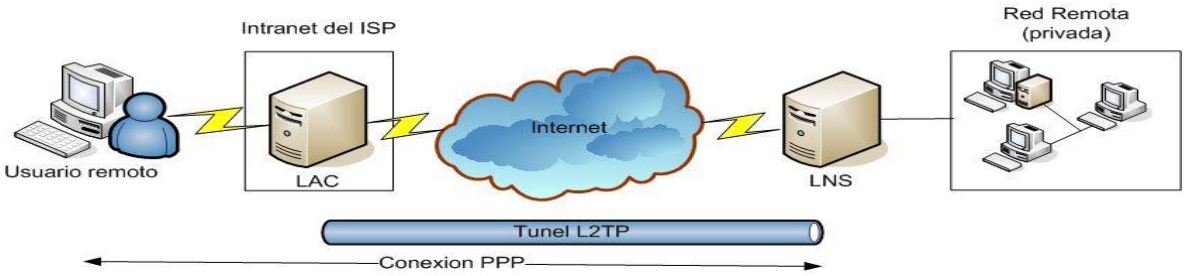


Figura 10.22 Túnel L2TP obligatorio

En le caso de los túneles L2TP obligatorios, el usuario final (cliente) es solo una entidad pasiva. Aparte de realizar la solicitud de conexión inicial el usuario final no juega otro papel en el proceso de establecimiento del túnel. Consecuentemente no ocurren mayores cambios en el lado del cliente L2TP.

Los túneles L2TP son considerados una mejor opción desde el punto de vista de la seguridad debido a que la conexión dial-up es utilizada en el lado del cliente para establecer la conexión PPP con el ISP. Como resultado el usuario final no puede acceder al Internet a menos que sea a través del gateway de la Intranet corporativa, lo cual permite a los administradores implementar mecanismos de seguridad como por ejemplo: restricciones, control de acceso y estrategias de medición.

Los pasos para el establecimiento de túneles L2TP obligatorios son:

- El usuario remoto hace una solicitud de conexión PPP desde el NAS localizado en el ISP.
- El NAS autentica al usuario. Este proceso de autenticación también ayuda al NAS a aprender acerca de la identidad del usuario que realiza la solicitud de conexión.
- Si el NAS es libre de aceptar la solicitud de conexión, un enlace PPP es establecido entre el ISP y el usuario remoto.
- El LAC inicia un túnel L2TP al LNS en la red anfitriona.

- Si la conexión es aceptada por el LNS, las tramas PPP atraviesan el túnel L2TP.
- El LNS acepta las tramas y obtiene las tramas PPP originales.
- Finalmente, el LNS autentica al usuario y los paquetes de datos recibidos. Si el usuario es validado satisfactoriamente, la IP apropiada es mapeada a la trama y luego enviada al nodo destino dentro de la intranet.

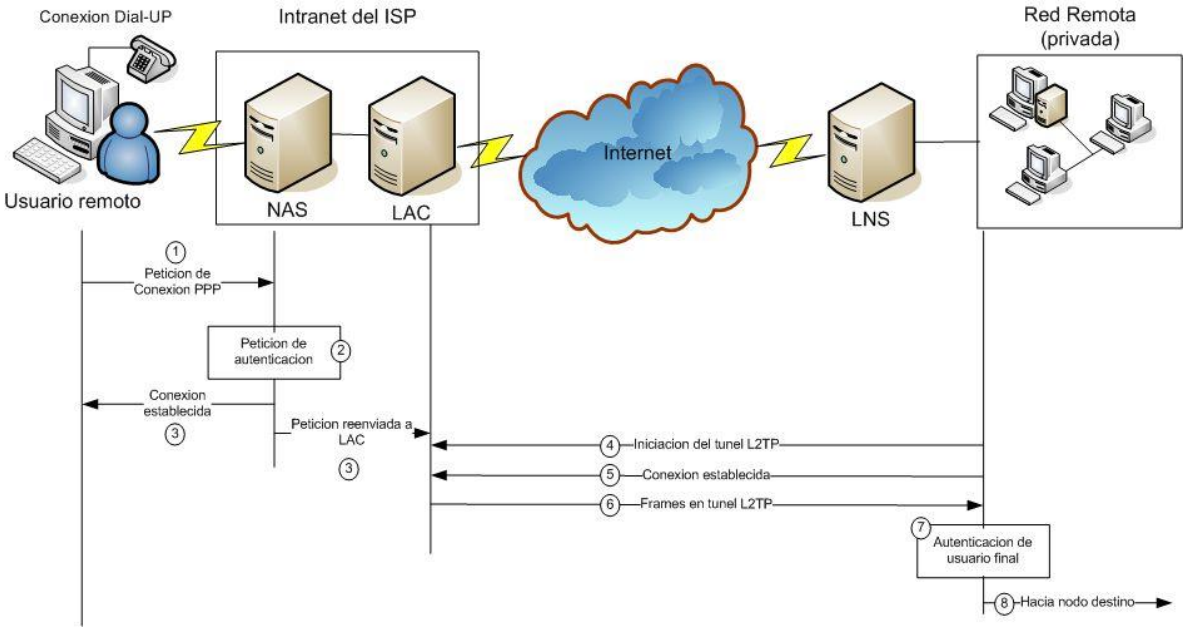


Figura 10.23 Estableciendo un túnel obligatorio

b. **Modo de túnel L2TP voluntario** Un túnel L2TP voluntario es establecido entre el usuario remoto y el LNS localizado en el lado de la red anfitriona. En este caso el usuario remoto actúa como el LAC. Como el papel que juega el ISP en el establecimiento de túneles L2TP voluntarios es mínimo, la infraestructura del ISP es transparente a los extremos que se comunican.

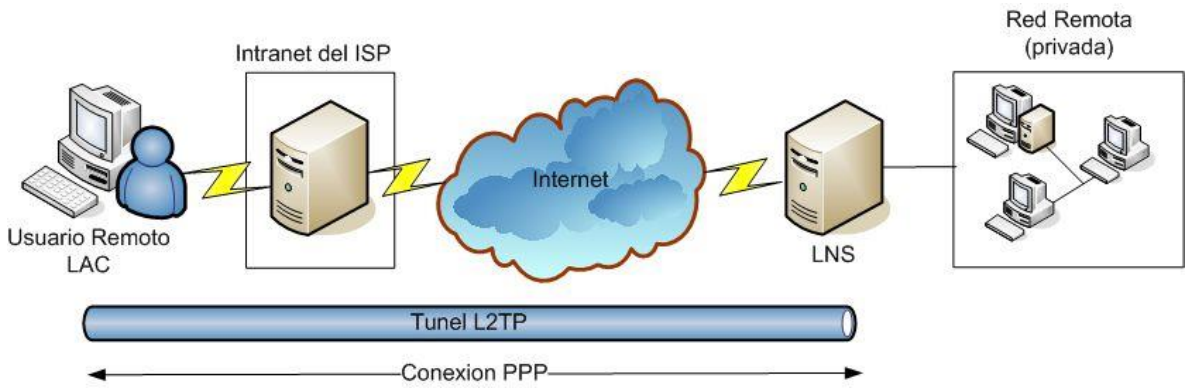


Figura 10.24 Túnel L2TP voluntario.

La ventaja más grande de utilizar túneles L2TP voluntarios es que permite a los usuarios remotos conectarse al Internet y establecer múltiples sesiones VPN simultáneamente. En cualquier caso, para poder utilizar este beneficio es necesario que el usuario remoto tenga asignadas múltiples direcciones IP. Una de estas direcciones IP es utilizada para realizar la conexión PPP al ISP y una dirección IP es utilizada para realizar cada una de las operaciones sobre el túnel L2TP. Pero este beneficio es también una desventaja, pues tanto el usuario remoto como la red anfitriona están expuestos a ser victimas de un ataque malicioso.

El establecimiento de túneles L2TP voluntarios es más simple que establecer un túnel L2TP obligatorio porque el usuario remoto utiliza una conexión PPP preestablecida. Los pasos involucrados en el establecimiento de un túnel L2TP voluntario son los siguientes:

- El LAC (En este caso el usuario remoto) lanza una solicitud para un túnel L2TP voluntario al LNS.
- Si la solicitud es aceptada por el LNS, el LAC envía las tramas PPP de acuerdo a las especificaciones L2TP, a través del túnel.
- El LNS acepta las tramas del túnel y procesa la información.
- Finalmente el LNS autentica la identidad del usuario y si el usuario es autenticado satisfactoriamente, envía las tramas al nodo destino dentro de la intranet.

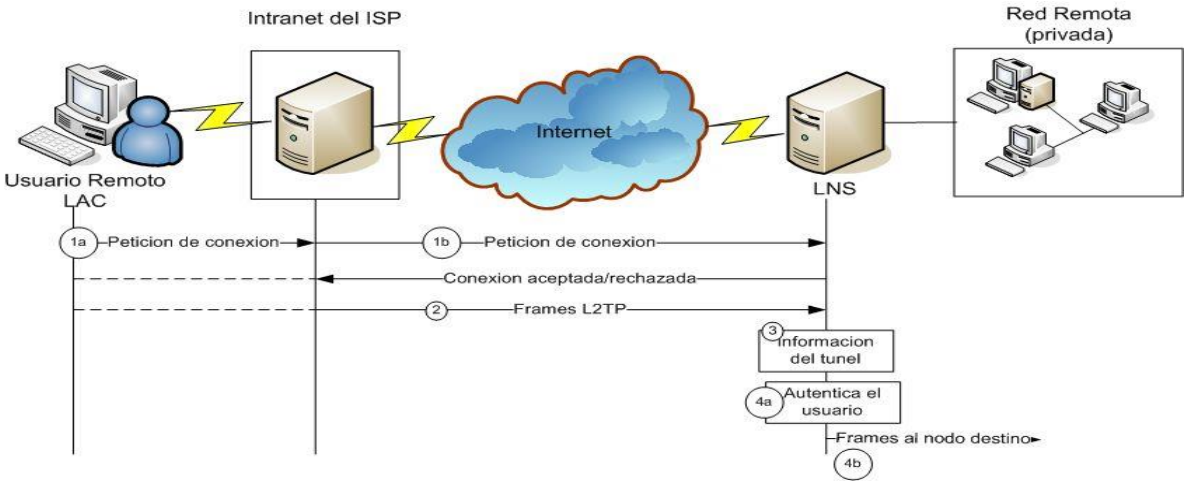


Figura 10.25 Un túnel L2TP voluntario

10.5.5 Control de conexión L2TP.

PPTP usa conexiones TCP separadas para el mantenimiento de túneles. Por otro lado la conexión de control L2TP y el mantenimiento de frames son basadas en UDP. El formato típico del mensaje de control L2TP es el siguiente:

Data Link Header	Ip Header	IPSec ESP Header	UDP Header	L2TP Message	IPSec ESP Trailer	IPSec ESP Authentication Trailer	Data Link Trailer

Figura 10.26 Formato del mensaje de control L2TP

Los datagramas UDP en los cuales se basan los mensajes de control L2TP, son de naturaleza desconectada. Esto implica que pueden ser entregados fuera de secuencia y no se produce acuse de recibo por parte del receptor cuando estos mensajes son entregados. Por esta razón L2TP emplea una técnica de secuenciamiento de mensajes. Esta técnica se asegura que los mensajes son entregados al destinatario en una secuencia. Dos campos de control especiales son utilizados como mensajes de control: Próximo recibido y próximo enviado, estos se aseguran que los mensajes son entregados en orden. Para mayor información acerca de los mensajes visitar http://www.faqs.org/rfcs/rfc2661.html

10.5.6 Seguridad en L2TP.

L2TP utiliza los métodos de autenticación de PPP para autenticar a sus usuarios. Los esquemas de autenticación L2TP comúnmente implementados son:

- PAP y SPAP
- EAP
- CHAP

Además de lo anteriormente mencionado, L2TP también utiliza IPSec para autenticar los paquetes de datos individuales. Esto reduce la velocidad de las transacciones pero asegura que los hackers y crackers no puedan tener oportunidades de violar la seguridad del túnel.

10.5.7 L2TP autenticado sobre IPSEC.

IPSec juega un papel importante en la seguridad de los paquetes L2TP. IPSec autentica los paquetes individuales aún después de que el usuario remoto ha sido autenticado satisfactoriamente.

10.5.8 Encriptación de datos L2TP.

L2TP a menudo utiliza ECP para la encriptación de datos. ECP es un protocolo que es utilizado para negociar un algoritmo de encripción, tal como DES, luego de que se ha establecido el enlace. Por lo tanto ECP ofrece capacidades avanzadas de encriptación adicionales a los mecanismos que ofrece PPP. Sin embargo la principal desventaja asociada a ECP es que las llaves una vez que han sido intercambiadas, no son refrescadas periódicamente. Esto incrementa la posibilidad de que un hacker pueda irrumpir y obtener las llaves y subsecuentemente en la transacción, durante una sesión de intercambio de datos prolongada. A continuación se ilustra como IPSec protege los tuneles L2TP voluntario y obligatorios.

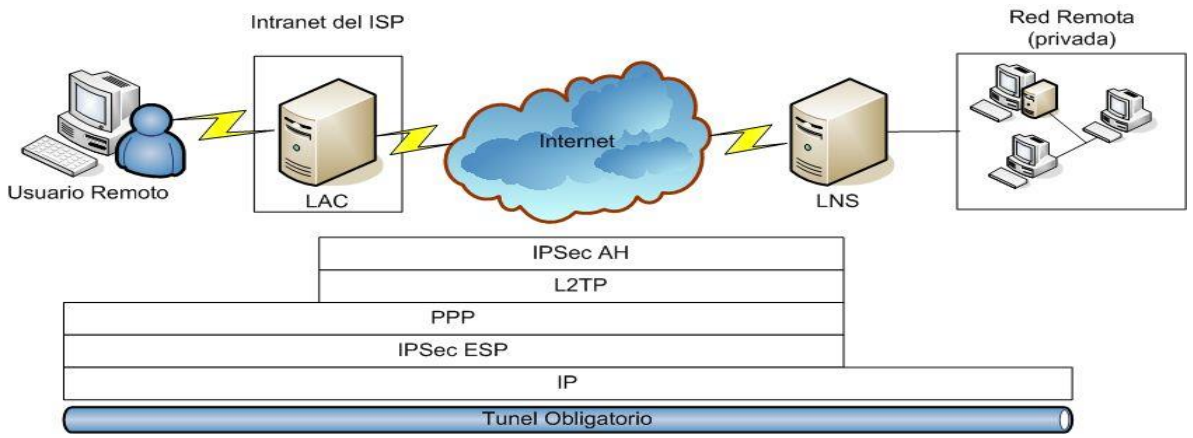


Figura 10.27 Protegiendo un túnel obligatorio usando IPSec

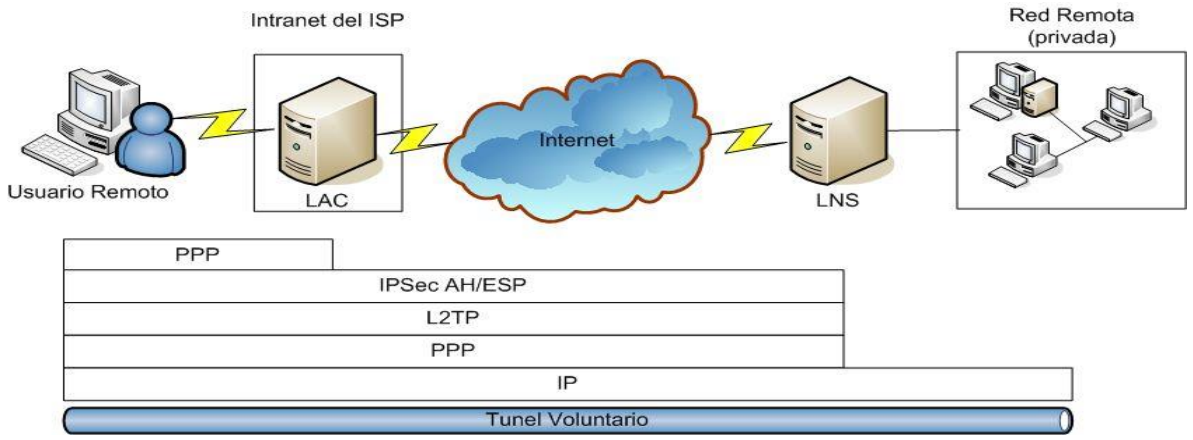


Figura 10.28 Protegiendo un túnel voluntario usando IPSec

10.5.9 Ventajas y desventajas de L2TP.

A continuación se presentan las principales ventajas que ofrece L2TP:

- L2TP es una solución genérica. En otras palabras es independiente de la plataforma. También soporta varias tecnologías de red. Además puede dar soporte a la transmisión de datos a través de enlaces WAN que no utilicen IP.
- Los túneles L2TP son transparentes al ISP tanto como al usuario remoto, por lo tanto no es requerida configuración adicional en el lado del ISP ni en el del cliente.

- L2TP permite a una corporación controlar la autenticación de un usuario en lugar del ISP.
- L2TP provee control de flujo y como resultado los paquetes pueden ser descartados arbitrariamente si el túnel se satura. Esto hace que las transacciones L2TP sean más rápidas que aquellas basadas en L2F.
- L2TP permite a un usuario remoto con una IP no registrada o privada acceder una red remota a través de una red pública.
- L2TP ofrece una seguridad incrementada debido al uso de IPSec.

La implementación de L2TP tiene algunas desventajas, entre las cuales se pueden mencionar:

- L2TP es más lento que PPTP o L2F debido a que utiliza IPSec para autenticar cada paquete recibido.
- PPTP se distribuye incluido en una solución VPN estándar de mercado. Un Servidor de Acceso Remoto y Ruteo requiere un gran proceso de configuración.

Resume de los tres protocolos para crear túneles VPN asociados a la capa de enlaces de datos.

características	**PPTP**	**L2F**	**L2TP**
Soporta múltiples protocolos	Si	Si	Si
Soporta múltiples enlaces PPP	No	Si	Si
Soporta múltiples conexiones de túneles	No	Si	Si
Modos de operación soportados	Entrante y saliente	Entrante	Entrante
Modos de tunes soportados	Voluntarios	Voluntarios y obligatorios	Voluntarios y obligatorios
Protocolo de transporte	IP/GRE	IP/UDP, IP/FR, IP/ATM	IP/UDP, IP/FR, IP/ATM

Protocolo de control	TCP, Port: 1723	UDP, Port: 1701	UDP, Port: 1701
Mecanismos de autenticación	MS-CHAP, PAP	CHAP, PAP, SPAP, EAP, IPSec, RADIUS y TACACS	CHAP, PAP, SPAP, EAP, IPSec, TACACS
Mecanismos de encriptación	MPPE	MPPE, IPSec	MPPE, IPSec, ECP

Tabla 10.5 resumen de los tres protocolos para elaborar un tune.

10.6. IPSEC (SEGURIDAD DEL PROTOCOLO INTERNET).

En la mayoría de las IOS de los Router soportan la suite de protocolos IPSec para habilitar características VPN avanzadas.

IPSec actúa en la capa de red, protegiendo y autentificando los paquetes IP entre un firewall y otros dispositivos participantes como: firewalls, routes, clientes VPN, hubs de la serie VPN 3000 y otros productos compatibles con IPSec.

IPSec habilita las siguientes características cuando se elabora una VPN:

- **Confidencialidad de datos.** El emisor lPSec puede cifrar paquetes antes de transmitirlos por una red.
- **Integridad de datos.** El receptor IPSec puede autentificar paquetes enviados por el emisor IPSec para garantizar que los datos no han sido alterados durante la transmisión. -
- Autenticación de origen de datos**.** El receptor lPSec puede autentificar el origen de los paquetes IPSec enviados. Este servicio depende del servicio de integridad de datos.
- **Antirreproducción.** El receptor IPSec puede detectar y rechazar paquetes reproducidos.

10.6.1. Visión general de IPSec.

IPSec es un marco de estándares abiertos que proporciona confidencialidad, integridad y autenticación de datos entre iguales participantes en la capa IP. Además puede usarse para proteger uno o más flujos de datos entre iguales IPSec. IPSec se basa en los dos siguientes protocolos:

- Cabecera de autenticación (AH).
- Sobrecarga de seguridad del encapsulado (ESP).

Además utiliza otros estándares de cifrado existentes para formar una *suite* de protocolos, los cuales son:

- Protocolo de seguridad IP.
    - Cabecera de autenticación (AH).
    - Sobrecarga de seguridad del encapsulado (ESP).

- Estándar de cifrado de datos (DES).
- Triple DES (3 DES).
- Diffie-Hellman (D-H).
- Boletín de mensajes 5 (MD5).
- Algoritmo *hash* seguro—1 (SHA-1).
- Firmas Rivest, Shamir y Alderman (RSA).
- Intercambio de clave de Internet (IKE).
- Autoridades de certificados (CA).

a. Protocolo de seguridad IP: Cabecera de autenticación (AH).

La cabecera de autenticación proporciona autenticación e integridad a los datagrarnas pasados entre dos sistemas.

Esto se logra aplicando una función tipo *hash* unidireccional con clave al datagrama para crear un boletín de mensajes. Si alguna parte del datagrama es modificada

durante el viaje, será detectada por el receptor cuando realice la misma función tipo *hash* unidireccional sobre el datagrama y compare el valor del boletín de mensajes que el emisor ha proporcionado. La operación hash unidireccional también implica el uso de un secreto compartido entre los dos sistemas, lo que significa que la autenticidad puede ser garantizada.

La AH puede también reforzar la protección antirreproductiva al requerir que un *host* receptor defina el bit de reproducción en la cabecera para indicar que el paquete ha sido visto. Sin esta protección, un atacante podría ser capaz de reenviar el mismo paquete muchas veces: por ejemplo, enviar un paquete que contenga "retirar 100 dólares de la cuenta X". La Figura 10.29 muestra dos *routers* y confirma que los datos entre ellos se envían en formato de sólo texto.

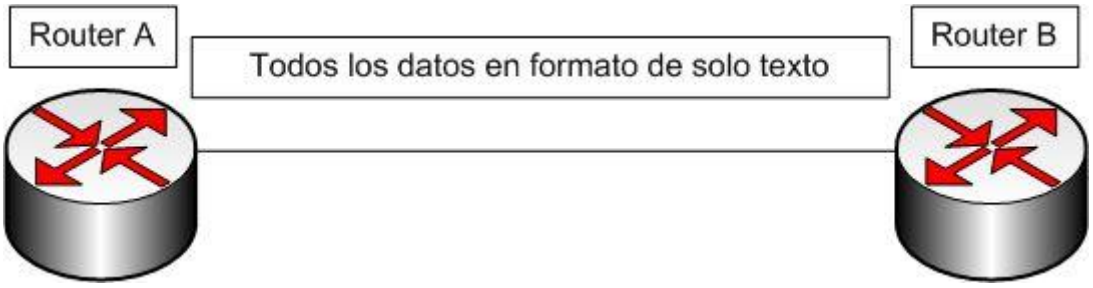


Figura 10.29 Cabecera de autenticación.

- Asegura la integridad de los datos.
- Proporciona autenticación de origen; asegura que los paquetes vinieron definitivamente del vecino.
- Utiliza un mecanismo *hash* con clave.
- NO proporciona confidencialidad (sin cifrado).
- Proporciona protección oficial de reproducción.

La función AH se aplica a todo el datagrama, exceptuando aquellos campos de la cabecera de IP mutables que cambien en tránsito, como por ejemplo, los campos Tiempo de existencia (TTL) que son modificados por los routers a lo largo de la ruta de transmisión. La AH funciona de la siguiente manera:

- Se aplica la función tipo *hash* a la cabecera de IP y la sobrecarga de datos.
- La función tipo *hash* se utiliza para construir una nueva cabecera AH, que se añade al paquete original.
- El nuevo paquete se transmite al vecino IPSec.
- El vecino aplica una función tipo *hash* a la cabecera de IP y la sobrecarga de datos, extrae el resultado de la función tipo *hash* transmitida desde la cabecera AH, y compara el resultado de las dos funciones *hash.* Los resultados de las f unciones tipo *hash* deben coincidir con exactitud. Incluso si un bit es cambiado en el paquete transmitido, la salida de la función tipo *hash* en el paquete recibido cambiará y la cabecera AH no coincidira.

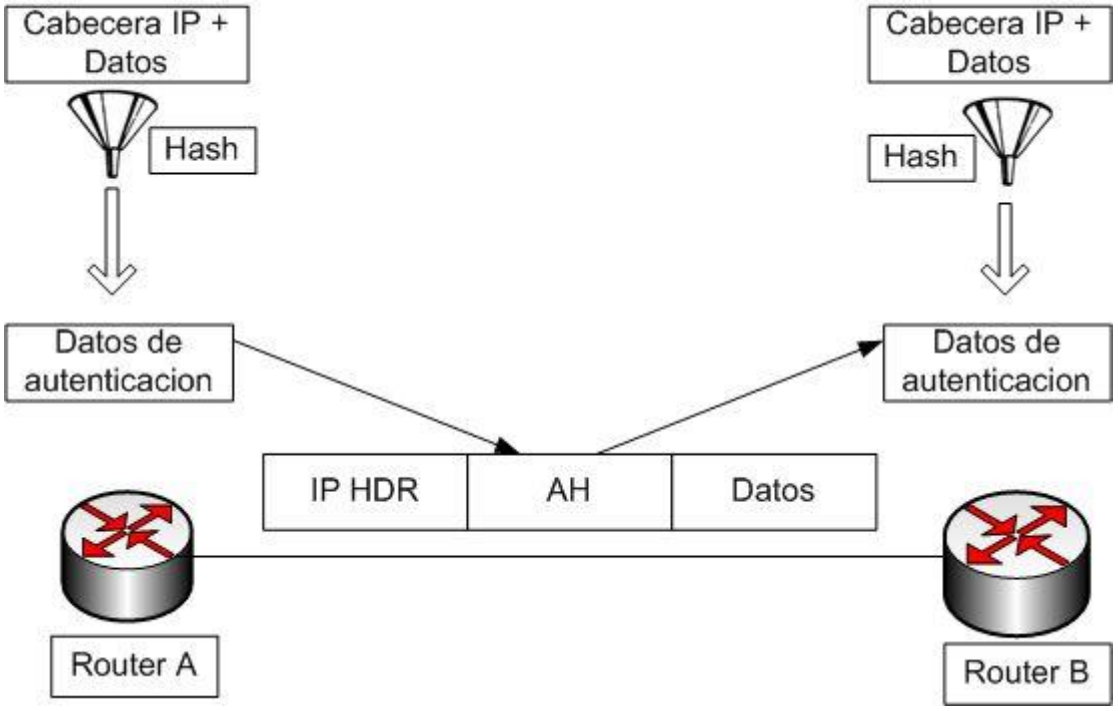


Figura 10.30 Autenticación e integridad de la AH.

b. Protocolo de seguridad IP: Sobrecarga de seguridad del encapsulado (ESP).

La sobrecarga de seguridad del encapsulado es un protocolo de seguridad usado para proporcionar confidencialidad (cifrado), autenticación del origen de los datos, integridad, servicio de antirreproducción (opcional) y confidencialidad del flujo de tráfico. La Figura 10.31 muestra que la sobrecarga de datos está cifrada con ESP.

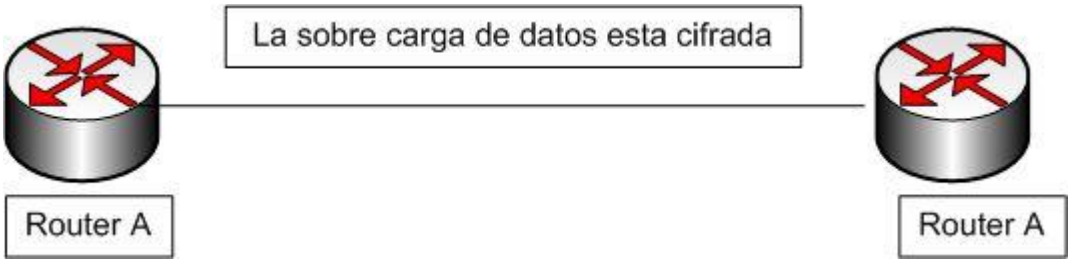


Figura 10.31. Sobrecarga de seguridad del encapsulado.

- Confidencialidad de datos (cifrado).
- Confidencialidad del flujo de tráfico limitado.
- Integridad de los datos.
- Autenticación opcional del origen de datos.
- Protección antirreproducción.
- No protege la cabecera de IP.

ESP proporciona confidencialidad realizando un cifrado en la capa del paquete IP. Soporta varios algoritmos de cifrado simétrico. El algoritmo predeterminado para IPSec es DES de 56 bits. Este código debe ser implementado para garantizar la interoperatividad entre los productos IPSec. Los productos Cisco también soportan el uso de 3DES para cifrado fuerte. La confidencialidad puede ser seleccionada independientemente de todos los demás servicios.

Al utilizar AH y ESP en una situación dada podría parecer complicado, pero puede simplificarse unas pocas reglas. Cuando se quiere asegurar que los datos de un origen autenticado se transfieren con integridad y no necesitan confidencialidad, se utiliza el protocolo AH. Si se necesita mantener la privacidad de los datos

(confidencialidad>, entonces se debe utilizar ESP. ESP cifrará los protocolos de la capa superior en modo transporte y todo el datagrama IP original en modo túnel para que ninguno sea legible desde el cable. Sin embargo, ESP también puede proporcionar ahora autenticación para los paquetes.

c. Algoritmo DES.

DES utiliza una clave de *56* bits, asegurando un cifrado de alto rendimiento. Se utiliza para cifrar y descifrar datos de paquetes. DES convierte texto normal en texto cifrado con un algoritmo de cifrado. El algoritmo de descifrado en el extremo remoto restablece el texto normal a partir del texto cifrado. Unas claves secretas compartidas posibilitan el cifrado y el descifrado.

d. Algoritmo triple DES (3 DES).

El algoritmo triple DES (3DES) es también un protocolo de cifrado soportados por los protocolos de Cisco para su uso en IPSec. El algoritmo 3DES opera de forma similar al DES en cuanto a que los datos se fragmentan en bloques de 64 bits. 3DES entonces procesa cada bloque tres veces, cada vez con una clave de 56 bits independiente. 3DES efectivamente duplica la fuerza de cifrado respecto al algoritmo DES de 56 bits.

e. Diffie-Hellman (D-H).

Diffie-Hellman (D-H) es un protocolo de cifrado de clave pública. Permite a dos partes establecer una clave secreta compartida usada por los algoritmos de cifrado DES o MD5, sobre un canal de comunicaciones inseguro. D-H se utiliza dentro del IKE para establecer claves de sesión. Los grupos D-H de 768 bits y 1024 bits son soportados en los rooters Cisco y los firewalls PIX. El grupo de 1024 bits es más seguro debido a que la clave es más grande.

f. Boletín de mensajes 5 (MD5).

MD5 es un algoritmo hash utilizado para autenticar los datos de un paquete. Los routers Cisco y los firewalls PIX utilizan la variante del código de autenticación de mensajes hash MD5 (HMAC) que proporciona un nivel adicional de la función tipo

hash. Una función tipo HASH es un algoritmo de cifrado unidireccional que torna como entrada un mensaje de longitud arbitraria y produce un mensaje de salida de longitud fija. IKE, AH y ESP utilizan MD5 para la autenticación.

g. Algoritmo HASH seguro —1 (SHA-1).

El algoritmo SHA-1 es un algoritmo hash utilizado para autenticar los datos de un paquete. Los reuters Cisco y los firewalls PIX utilizan la variante HMAC de SHA-1, que proporciona un nivel hash adicional. IKE, AH y ESP utilizan SHA-1 para la autenticación.

h. Firmas Rivest, Shamir y Alderman (RSA).

Rivest, Shamir y Alderman (RSA) es un sistema criptográfico de clave pública usado para la autenticación. El IKE de los reuters Cisco o los firewalls PIX utiliza un intercambio D-H para determinar las claves secretas de cada IPSec utilizadas por los algoritmos de cifrado. El intercambio D-H puede ser autenticado con firmas RSA o claves precompartidas.

i. Intercambio de clave de Internet (IKE).

El Intercambio de clave de Internet (IKE) es un protocolo híbrido que proporciona servicios de utilidad para IPSec: autenticación de los iguales IPSec, negociación de las asociaciones de seguridad del IKE e IPSec, y establecimiento de claves para algoritmos de cifrado usados por IPSec.

Nota: KE es sinónimo del Protocolo de administración de clave de la asociación para la seguridad en Internet (ISAKMP) en las configuraciones router Cisco o firewall PIX.

j. Autoridades de certificados (CA).

La Autoridad de certificados (CA) ofrecida por los *reuters* y los *ftrewalls* permite a la red protegida con IPSec escalar proporcionando el equivalente de una tarjeta de identificación digital a cada dispositivo. Cuando dos puntos IPSec desean

comunicarse, iritercambian certificados digitales para demostrar sus identidades eliminando así la necesidad de intercambiar claves públicas manualmente con cada punto o de especificar una clave compartida manualmente en cada punto. Los certificados digitales se obtienen de una CA. El soporte CA en los productos Cisco utiliza firmas RSA para autenticar el intercambio.

10.6.2. Modos túnel y transporte.

lPSec puede ejecutarse en nodo túnel o en modo transporte. Cada uno de estos modos tiene sus propios usos particulares. El modo transporte debería usarse para sesiones de extremo a extremo y el modo túnel debería usarse para todo lo demás.

El modo túnel se usa con más frecuencia entre gateway o desde una estación final hasta un gateway. El gateway actúa como proxy para los hosts subyacentes. El modo transporte se usa entre estaciones finales o entre una estación final y un gateway, si este último está siendo tratado como h*ost;* por ejemplo, en una sesión Telnet cifrada desde una estación de trabajo hasta un *router,* el router es el destino real.

La figura 10.31 es utilizada como referencia para algunos ejemplos de cuando usar el modo túnel o el modo transporte.

Ejemplo A. El modo túnel se utiliza normalmente para cifrar tráfico entre gateways lPSec seguros, como entre un router firewall, como se muestra en el Ejemplo de la figura 10.31 Los gateways lPSec actúan como proxy lPSec para los dispositivos subyacentes, como la PC1 y los servidores HR de la figura. En el Ejemplo A, PC1 se conecta a los servidores HR con seguridad a través del túnel íPSec instalado entre los gateways.

Ejemplo B. El modo túnel también se usa para conectar una estación final que ejecuta software lPSec, como el cliente para VPN y un gateway lPSec,

Ejemplo C. El modo túnel se usa para instalar un túnel IPSec entre el router y un servidor que ejecuta software IPSoc. El software Cisco los y el firewall definen el modo túnel como el modo IPSec predeterminado.

Ejemplo D. El modo transporte se usa entre estaciones finales que soportan IPSec o entre una estación final y un gateway si éste está tratándose como host. En el Ejemplo D, el modo transporte se usa para instalar una sesión Telnet cifrada desde el PC1 que ejecuta el software cliente VPN para terminar en firewall, posibilitando a PC1 configurar remotamente el firewall de forma segura.

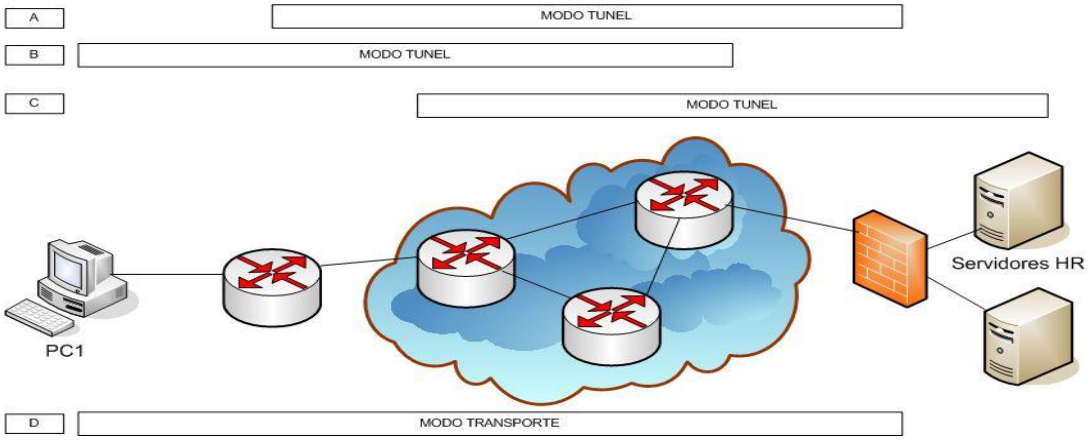


Figura 10.31 IPSec en modo tunel y modo transporte.

10.6.3 Modo túnel frente a modo transporte en AH.

La Figura 10.32 muestra las diferencias que el modo IPSec registra en AH. En el modo transporte, los servicios AH protegen la cabecera IP externa, así como la sobrecarga de datos. Los servicios AH protegen todos los campos de la cabecera que no cambian durante el transporte. La AH va después de la cabecera de IP y antes de la cabecera ESP, si está presente, y de los otros protocolos de capa superior.

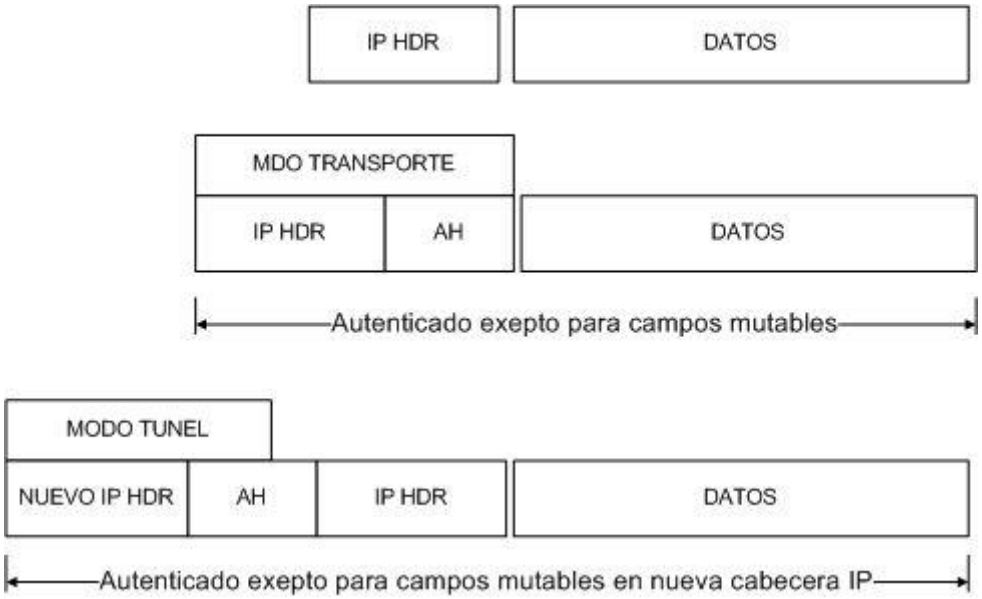


Figura10.32 modo túnel modo frente a modo transporte.

En el modo túnel, toda la cabecera original es autenticada, se construye una nueva cabecera de IP, y la nueva cabecera de IP es protegida de la misma manera que la cabecera IP en el modo transporte.

AH es incompatible con la Traducción de direcciones de red (NAT) porque NAT cambia la dirección IP de origen, lo que romperá la cabecera AH y causará que los paquetes sean rechazados por el IPSec.

10.6.4. Túnel ESP frente a modo transporte.

La Figura 10.33 muestra las diferencias que el modo IPSec registra en ESP. En el modo transporte, la sobrecarga de IP está cifrada y las cabeceras originales se dejan intactas. La cabecera ESP se inserta después de la cabecera de IP y antes de la cabecera del protocolo de capa superior. Los protocolos de capa superior son cifrados y autenticados junto con la cabecera ESP. ESP no autentica la propia cabecera de IP. La información de la capa superior no está disponible porque es parte de la sobrecarga cifrada.

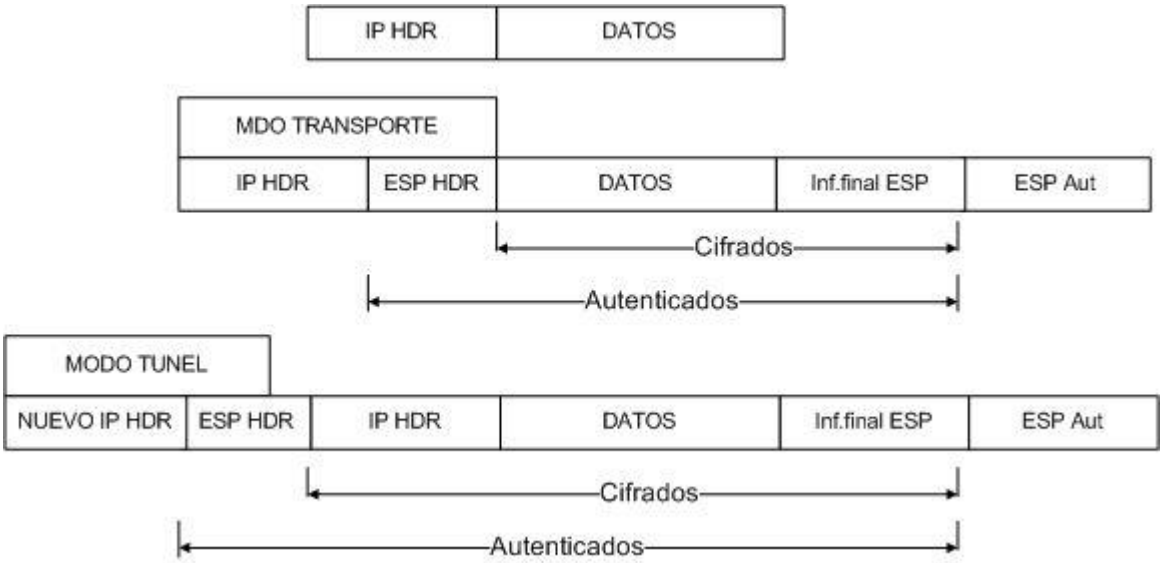


Figura 10.33 Modo túnel ESP frente a modo transporte

Cuando se usa ESP en modo túnel, la cabecera IP original está bien protegida porque todo el datagrarna IP original está cifrado con un mecanismo de autenticación ESP, se incluyen el datagrama IP original y la cabecera ESP; sin embargo, la nueva cabecera IP no está incluida en la autenticación.

El cifrado se realiza primero, antes que la autenticación. Una razón para este orden de procesamiento es que: facilita la detección rápida y el rechazo de paquetes reproducidos o falsos por parte del nodo receptor. Antes de descifrar el paquete, el receptor puede detectar el problema y reducir potencialmente el impacto de los ataques de denegación de servicio.

ESP también puede proporcional autenticación de paquetes con un campo adicional para la autenticación. El software Cisco IOS y los Firewall PIX se refieren a este servicio como ESP HMAC. La autenticación se calcula después de efectuar el cifrado. El estándar lPSec actual específica SHA-1 y MD5 como los algoritmos HMAC obligatorios.

La diferencia principal entre la autenticación proporcionada por ESP y la proporcionada por AH es la extensión de la cobertura. ESP no protege ninguno de

los campos do una cabecera IP a menos que esos campos estén encapsulados por ESP modo túnel. La Figura 1 ilustra los campos protegidos por ESP HMAC.

- Proporciona confidencialidad ESP con cifrado
- Proporciona integridad con HMAC con clave.

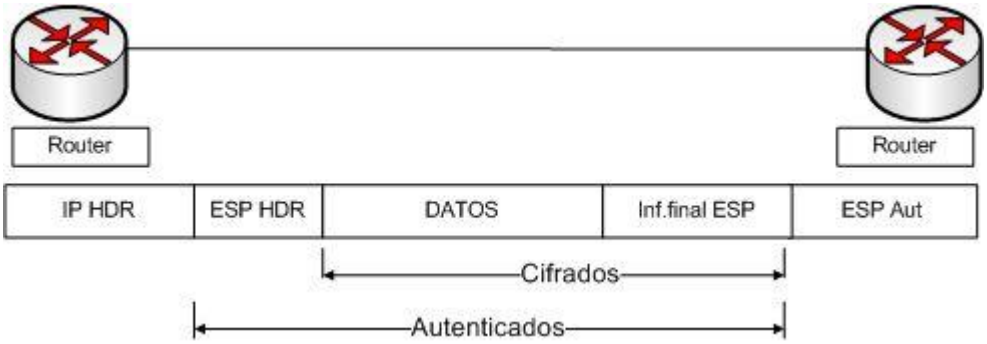


Figura 10.34 Cifrado ESP con un HMAC con clave.

10.6.5 . Transformaciones IPSec

Una transformación IPSec especifica un solo protocolo de seguridad IPSec AH o ESP con sus correspondientes algoritmos de seguridad y modos. Algunos ejemplos de transformaciones incluyen lo siguiente:

- El protocolo AH con el algoritmo de autenticación HMAC con MD5 en modo túnel se usa para la autenticación.
- El proceso ESP con el algoritmo de cifrado 3DES en modo transporte se usa para la confiabilidad de los datos

El protocolo ESP con el algoritmo de cifrado DES de 56 bits y el algoritmo de autenticación HMAC con SHA en modo túnel se usan para la autenticación y la confidencialidad.

10.6.6 Conjuntos de transformación.

Un conjunto de transformación es una combinación de transformaciones IPSec individuales diseñadas para establecer una norma de seguridad específica para el tráfico. Durante la negociación de la asociación de seguridad IPSec ISAKMP que ocurre en el modo rápido de la fase 2 del IKE, los iguales acuerdan usar un conjunto de transformación particular para proteger un flujo de datos concreto. Los conjuntos de transformación combinan los siguientes factores de IPSec:

- Mecanismo para la autenticación de la sobrecarga. Transformación AH.
- Mecanismo para cifrado de la sobrecarga. Transformación ESP.
- Modo IPSec (transporte frente a túnel).

Los conjuntos de transformación son iguales a una combinación de una transformación AH, una transformación ESP y el modo IPSec (modo túnel o transporte).

10.6.7 Componentes del cifrado Ipsec.

A continuación se describen las tecnologías de componentes utilizadas en IPSec:

a. Cifrado DES.

Los componentes del cifrado DES son los siguientes: Algoritmos de cifrado y descifrado, Emparejamiento de claves secretas compartidas.y entrada de datos en formato de sólo texto para ser cifrados.

En el centro de DES esta el algoritmo de cifrado, Una clave secreta compartida es la entrada del algoritmo. Los datos en formato de solo texto son suministrados al algoritmo en bloques de longitud fija y convertidos en texto cifrado. El texto cifrado es transmitido al IPSec utilizando ESP. El IPSec recibe el paquete ESP, extrae el texto cifrado, lo pasa a través del algoritmo de descifrado y como salida se obtiene el texto idéntico al introducido en el cifrado. El algoritmo de cifrado DES puede verse en la figura 10.35.

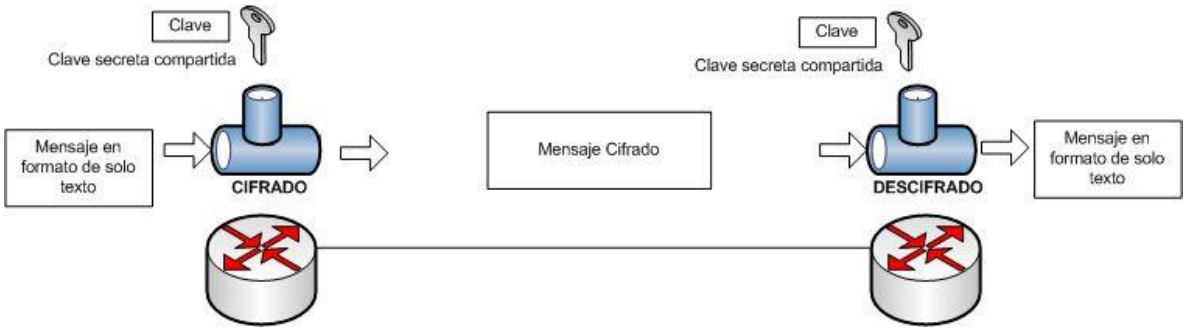


Figura 10.35 cifrado DES

- El cifrado convierte el texto normal en texto cifrado.
- El descifrado recupera el texto normal a partir del texto cifrado
- Las claves posibilitan el cifrado y el descifrado

b. Acuerdo de clave Diffie-Hellman (D-H).

El acuerdo de clave Diffie-Hellman (D-H) es un método de cifrado de clave pública que proporciona una forma para que dos router IPSec establezcan una clave secreta compartida que sólo ellos conocen, aunque se estén comunicando sobre un canal inseguro.

Con D-H, cada IPSec genera un par de claves, una pública y otra privada. La clave privada generada por cada IPSec es mantenida en secreto y nunca es compartida. La clave pública es calculada a partir de la clave privada por cada router y es intercambiada sobre el canal inseguro. Cada router combina la clave pública del otro con su propia clave privada y computa el mismo número secreto compartido. Este último se convierte después en una clave secreta compartida, clave que nunca es intercambiada sobre el canal inseguro.

Como se puede ver en la Figura 10.36. el intercambio dc clave Díffie-Hellnian es un proceso complicado. Esto contribuye a la efectividad del algoritmo de cifrado.

NOTA: Diffie-Hellman es muy importante porque la clave secreta compartida se usa para cifrar datos utilizando los algoritmos de cifrado de la clave secreta especializados en Las asociaciones de seguridad IPSec, como DES o MDS.

Figura 10.36. Acuerdo de clave Diffie-Hellman

1. Generar un número entero p
   enviar p al router 2
   generar g
2. Generar la clave privada X_A
3. Generar clave publica
   $Y_A = g^{\wedge}X_A$ mop p
4. Enviar clave pública Y_A
5. Generar numero secreto
   compartido $ZZ = Y_B{\wedge}X_A$ mop p
6. Generar clave secreta compartida
   A partir de ZZ (56 bits para DES
   168 bits para 3DES)

1. Generar un número entero q
   recibir q del router 1
   generar g
2. Generar clave privada
3. Generar clave pública
   $Y_B = g^{\wedge}X_B$ mop p
4. Enviar clave pública Y_B
5. Generar numero secreto
   compartido $ZZ = Y_A{\wedge}X_B$ mop p
6. Generar clave secreta
   compartida A partir de ZZ
   (56 bits para DES
   168 bits para 3DES).

El proceso Diffie-Hellman El proceso Diffie-Hellman es el siguiente:

Paso 1 El proceso Diffie-Hellman empieza con cada router generando un número entero primo grande, p y q. Cada router envía al otro su número entero primo sobre el canal inseguro. Por ejemplo, el router1 envía p al router2. Después, cada router utiliza los valores p y q para generar g, una raíz primitiva de p.

Paso 2 Cada router genera una clave D-H privada (router1: Xa, router2: Xb).

Paso 3 Cada router genera una clave D-H pública. La clave privada local se combina con el número primo p y la raíz primitiva g en cada router para generar una clave pública: Ya para el router1 e Yb para el router2. La fórmula para el router1 es Ya=gAXa mod p. La fórmula para el router2 es Yb=gAXb mod p. La exponenciación es computacionalmente cara. El carácter A denota la exponenciación (gAxa es g a la potencia Xa); mod extrae el coeficiente.

Paso 4 Las claves públicas Ya e Yb son intercambiadas públicamente.

Paso 5 Cada router genera un número secreto compartido (ZZ) combinando la clave pública recibida desde el router opuesto con su propia clave privada. La fórmula para el router1 es ZZz(YbXa) mod p. La fórmula para el router2 es ZZ=(YaXb) mod p. Los valores ZZ son idénticos en cada router. Cualquiera que conozca p o g, o las claves públicas D-H, no puede adivinar o calcular fácilmente el valor secreto compartido, principalmente a causa de la dificultad que supone descomponer en factores números primos grandes.

Paso 6 Las claves secretas compartidas derivan del número secreto compartido ZZ para su uso por parte de DES o HMAC.

NOTA: Cada router IPSec tiene tres claves:

- una clave privada que es mantenida en secreto y nunca es compartida. Se utiliza para firmar mensajes.
- Una clave pública compartida. La utilizan otros para verificar una firma.
- una clave secreta compartida que se utilizada para cifrar datos usando un algoritmo de cifrado DES, MD5, entre otos. La clave secreta compartida se deriva de la generación de la clave Diffie-Hellman.

c. HMAC

Los algoritmos hash usados por IPSec son funciones seguras tipo hash M D5 y SHA1 Los algoritmos hash han evolucionado hasta los HMAC, que combinan la seguridad demostrada de los algoritmos hash, Con funciones criptográficas adicionales. El resultado de la función tipo HASH, es cifrado con la clave privada del emisor dando como resultado una suma de comprobación con clave como salida.

En la Figura10.37 la función; tipo HASH torna como entrada los datos en formato de sólo texto, de longitud variable que e necesitan ser autenticados y una clave privada es la misma que la de salida de la función tipo HASH. El algoritmo HMAC se ejecuta**,** con una suma de comprobación resultante de longitud fija como de salida. Este valor de la suma de comprobación se envía con el mensaje en forma firma. El igual receptor ejecuta un HMAC sobre los mismos datos de mensajes que fueron introducidos en el emisor usando la misma clave privada, y el resultado de la función tipo HASH resultante es comprobado con el resultado de la función tipo HASH recibido, el resultado final tendría que ser el mismo exactamente.

Figura 10.37 codigo de autenticación de mensaje HASH (HMAC).

d. HMAC-MD5-96.

La técnica de cifrado HMAC-MD5-96 (también conocida como HMAC-MD5) es usada por IPSec para garantizar que un mensaje no ha sido alterado. HMAC-MD5 utiliza la función tipo hash, MD5 desarrollada por Ronald Rivest, del Instituto de Tecnología de Massachusetts, y RSA Data Security Incorporated, la cual está descrita en la RFC 1321.

HMAC-MD5 usa una clave secreta de 128 bits. Produce un valor autenticado de 128 bits. Este valor de 128 bits es truncado en los primeros 96 bits. Al enviar, el valor truncado este es almacenado dentro del campo autenticador de AH o ESP —HMAC. Al recibirlo, se computa el valor de 128 bits en su totalidad, y los primeros 96 bits se comparan con el valor almacenado en el campo autenticador.

En MD5 se ha demostrado recientemente que es vulnerable a los ataques de búsqueda de colisión. Este ataque y otras debilidades actualmente conocidas de MD5 no comprometen el uso de MD5 dentro de HMAC, ya que no se ha demostrado ningún ataque conocido contra HMAC—MD5.

e. HMAC-SHA-1 –96.

La técnica de cifrado HMAC-SHA-1 –96 también conocida como HMAC-SHA-1 es

usada por IPSec para garantizar que un mensaje no ha sido alterado. HMAC-SHA-1 usa el SHA- 1 especificado en FIPS-190-1, combinado con HMAC (como el cual esta descrito en el RFC 2404.

HMAC-SHA-1 usa una clave secreta de 160 bits. Produce un valor autenticador de 160 bits. Este valor de 160 bits es truncado en los primeros 96 bits. Al enviar, el valor truncado es almacenado dentro del campo autenticador de AH o ESP-HMAC. Al recibir, se computa el valor de 160 bits en su totalidad, y los primeros 96 bits se comparan con el valor almacenado en el campo autenticador.

SHA-1 está considerado más fuerte criptograficamente que MD5 sin embargo, necesita más ciclos de CPU para su computación.

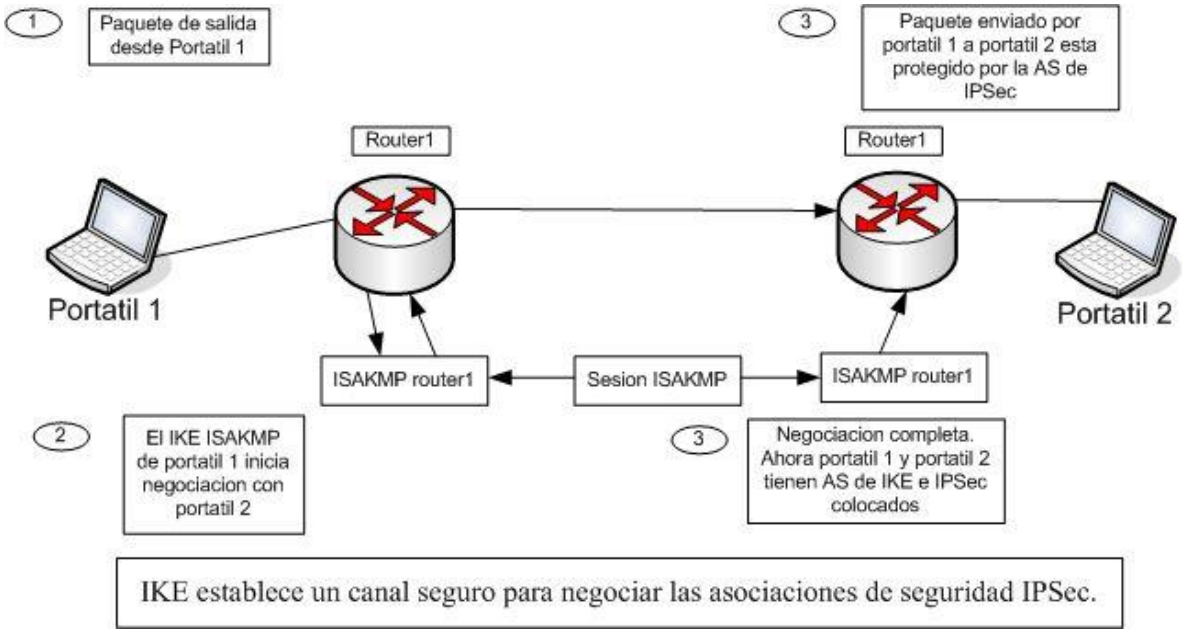
10.6.8 Visión general del IKE.

El IKE negocia las asociaciones de seguridad (AS) de IPSec. Este proceso requiere que los sistemas IPSec primero se autentiquen entre sí y establezcan las claves compartidas ISAKMP.

En la fase uno, IKE crea un canal seguro autenticado entre los dos router IKE que se llama Asociación de seguridad IKE. El acuerdo de clave Diffie-Hellman siempre se realiza en esta fase.

En la fase dos, el IKE negocia las asociaciones de seguridad IPSec y genera el material de clave necesario para IPSec. El emisor ofrece uno o más conjuntos de transformación que se usan para especificar una combinación permitida de transformaciones con sus respectivas configuraciones. El emisor también indica el flujo de datos a los que el conjunto de transformación tiene que ser aplicado. El emisor debe ofrecer por lo menos un conjunto de transformación. El receptor entonces envía de vuelta un solo conjunto de transformación, que indica las transformaciones y algoritmos acordados mutuamente para esta sesión IPSec en

particular. En la fase dos puede efectuarse un nuevo acuerdo Diffie-Hellman, o las claves pueden ser derivadas de la llave secreta compartida de la fase uno.



La figura 10.38 la función del IKE

NOTA**:** Una asociación de seguridad (AS) es una relación entre dos o más entidades que describe cómo las entidades usarán los servicios de seguridad para comunicarse de forma segura.

El IKE autentica los mensajes del router y de IKE entre los routers durante la fase uno del IKE. La fase uno consta de dos modos el principal o el agresivo. Los routers potenciales en una sesión IPSec deben autenticarse a sí mismos ante el otro antes de que el IKE pueda proceder. La autenticación del router ocurre durante el intercambio en modo principal que se da en la fase uno del IKE. El protocolo IKE es muy flexible y soporta múltiples métodos de autenticación como parte del intercambio de la fase uno. Las dos entidades deben acordar un protocolo común de autenticación a través de un proceso de negociación. La fase uno del IKE para autenticar router IPSec tiene tres métodos los cuales son:

- **Claves precompartidas.** Un valor clave introducido en cada router manualmente (out-of-band) usado para autenticar al router.

- **Firmas RSA.** Usan un certificado digital autenticado por una firma RSA.
- **Números aleatorios cifrados RSA.** Usan cifrado RSA para cifrar un valor ocasional (un número aleatorio generado por el router) y otros valores.

Un valor común usado por todos los métodos de autenticación es la identidad del router (ID), que ayuda a identificar el router. Algunos valores ID usados son los siguientes:

- Dirección IP del router *(cuatro octetos),* como por ejemplo 172.30.2.2.
- Nombre de dominio completamente cualificado (FQDN), como por ejemplo egresados@tesis.com.sv.

a. Claves precompartidas.

Con claves precompartidas, la misma clave precompartida es configurada en cada Router. Los router del IKE se autentican el uno al otro computando y enviando una función tipo hash con clave de datos que incluye la clave precompartida. Si el router receptor es capaz de crear la misma función tipo *hash* independientemente usando su clave precompartida, sabe que ambos router deben compartir la misma clave secreta, autenticando así al otro router.

Las claves precompartidas son más fáciles de configurar que configurar manualmente valores de norma IPSec en cada IPSec. Sin embargo, las claves precompartidas no son escalables porque cada router lPSec debe ser configurado con la clave precompartida de cada uno de los otros router con los que establecerá una sesión.

b. Firmas RSA

El método de firmas RSA utiliza una firma digital, donde cada dispositivo firma digitalmente un conjunto de datos y los envía a la otra parte. Las firmas RSA usan una CA para generar un único certificado digital de identidad que es asignado a cada router para su autenticación. El certificado de identidad digital es similar en cuanto a su función a la clave precompartida, pero proporciona una seguridad mucho más fuerte.

RSA es un sistema de cifrado de clave pública usado por IPSec para la autenticación en la fase 1 deI *IKE.* RSA fue desarrollado en 1977 por Ronald Rivest, Adi Shamir y Leonard Adelman.

El iniciador y el contestador a una sesión IKB usando firmas RSA envían su propio valor ID (IDi, IDr), su certificado digital de identidad, y un valor de firma RSA consistente en una variedad de valores IKE, todos cifrados mediante el método de cifrado que utilizara IKE (DES o 3DES).

c. Cifrado RSA

El método de los números aleatorios cifrados RSA usa *e*l estándar de criptografía de clave pública de cifrado RSA. El método requiere que cada parte genere un número pseudoaleatorio y lo cifre en la clave privada RSA de la otra parte. La autenticación se produce cuando cada parte descifra el valor aleatorio de la otra parte con una clave privada usando el número aleatorio descifrado para computar una función tipo hash con clave.

10.6.9 Funcionamiento de IPSEC.

IPSec tiene muchas tecnologías de componentes y métodos de cifrado. Sin embargo, el funcionamiento de IPSec puede ser fragmentado en cinco pasos principales que a continuación se resumen:

Paso 1 Un tráfico de interés inicia el proceso IPSec. El tráfico se considera interesante cuando la norma de seguridad IPSec configurada en los router IPSec comienza el proceso del IKE.

Paso 2 Fase uno del IKE. El IKE autentica a los router que utilizan IPSec y negocian las AS de IKE durante esta fase, instalando un canal seguro para negociar las AS de lPSec en la fase dos.

Paso 3 Fase dos del IKE. El JKE negocia los parámetros de las AS de IPSec e instala las AS de IPSec coincidentes en los router.

Paso 4 Transferencia de datos. Los datos son transferidos entre los router que utilizan IPSec en base a los parámetros IPSec y las claves almacenadas en la base de datos de la AS.

Paso 5 Terminación del túnel lPSec.

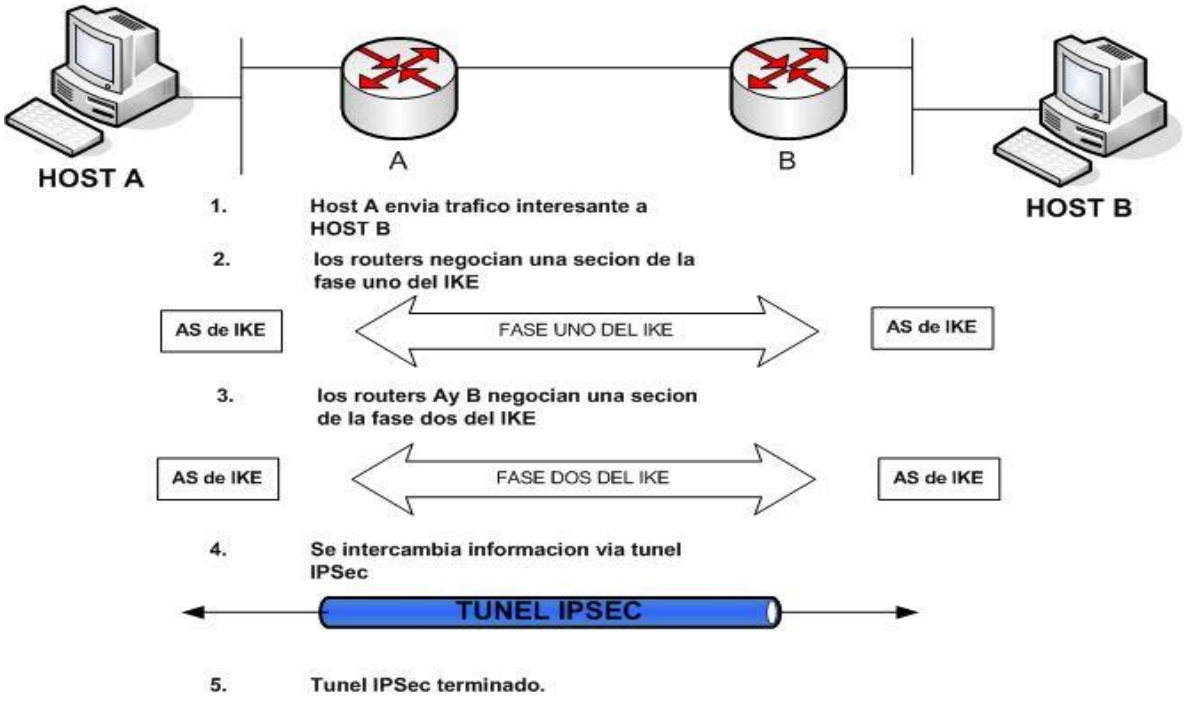


Figura 10.40. Los cinco pasos del IPSec.

Para mayor información acerca de las fases del protocolo IKE visitar la página http://www.faqs.org/rfcs/rfc2409.html

10.6.10 Asociaciones de seguridad (AS) de ipsec.

El concepto de una asociación de seguridad (AS) es fundamental para IPSec. Una AS es una relación entre dos o más entidades. La AS describe cómo las entidades usarán los servicios de seguridad para comunicarse de forma segura. IPSec

proporciona muchas opciones para realizar cifrado de red y autenticación. Cada conexión IPSec puede proporcionar cifrado, integridad, autenticidad, o las tres. Cuando el servicio de seguridad está determinado los dos router IPSec deben determinar exactamente qué algoritmos utilizar (por ejemplo; DES o 3DES para cifrado, MD5 o SHA para integridad). Después de decidir sobre los algoritmos, los dos dispositivos deben compartir claves de sesión. La asociación de seguridad es el método que IPSec utiliza para seguir todos los detalles que conciernen a una sesión IPSec dada.

NOTA**:** La nomenclatura resulta un poco confusa a veces, porque las AS no sólo se utilizan para lPSec. Por ejemplo, las AS de IKE describen los parámetros de seguridad entre dos dispositivos IKE.

10.6.11 Cuadro de flujo del IKE e IPSEC.

El software lOS de los router que soportan IPSec pone en ejecución y procesa AS de un modo predecible y fiable. En la figura 10.45. Se muestra un resumen de cómo funciona IPSec en el software lOS de un router. El proceso mostrado en esta figura se asume que ya se han creado las propias claves públicas y privadas y que como mínimo existe una lista de acceso La figura 1.23 también muestra los comandos del software IOS usados para configurar cada parte del proceso auque los comandos no se muestran en el orden en el que deben introducirse.

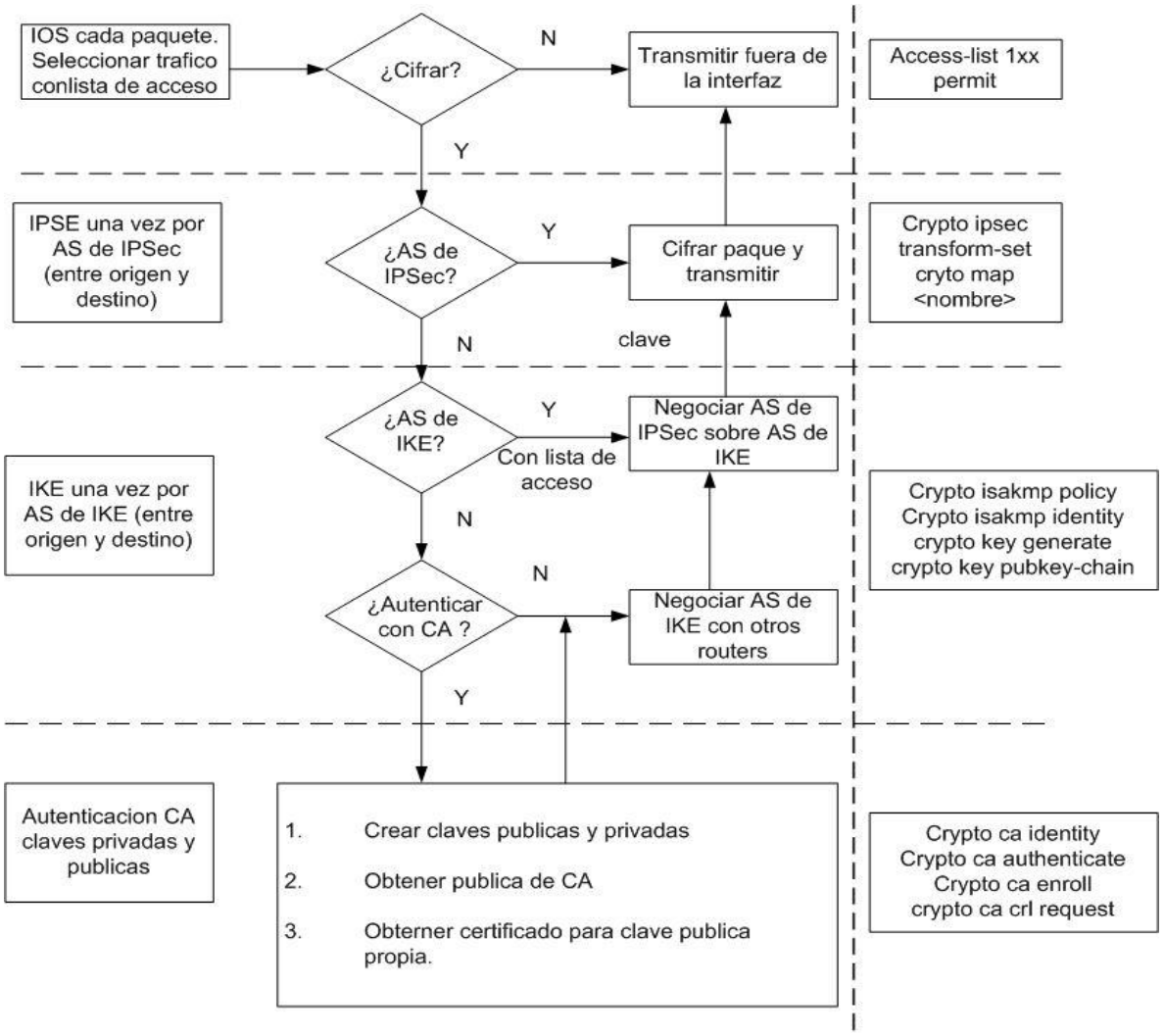


Figura10.45 cuadro de flujo IKE e IPSec.

NOTA: IKE es sinónimo de ISAkMP en las configuraciones de los routers CiSCO o los pixfirewall.

CAPITULO 11. VPN.

El reto es el mismo cuando se intercambia información de un sitio a otro: ¿cómo se puede transferir la información de forma segura?

En este capitulo se presentan las VPN como parte de la estrategia de seguridad “Defensa en profundidad” y como estas ayudan a cubrir la necesidad planteada anteriormente. Las VPN hacen uso de otras tecnologías como firewalls y routers a los cuales integra para un mismo propósito de brindar integridad, disponibilidad y confidencialidad de los recursos de una red.

Puntos clave

- Entender que es un VPN
- Conocer porque son importantes
- Detallar las ventajas que se obtienes al usar VPN
- Proveer de algunos esquemas y clasificaciones de VPN basado en diferentes enfoques
- Proporcionar de criterios de elección de tecnologías de VPN.

11.1. VISIÓN GENERAL DE LAS VPN.

Siempre ha habido una división evidente entre red pública y red privada, como el sistema telefónico público y la Internet, es una gran colección de usuarios que intercambian información unos con otros más o menos libremente.
Una red privada está compuesta de computadoras propiedad de una simple organización que comparten información específicamente una con otra. Se aseguran que vayan a ser los únicos usando la red, y que la información enviada entre ellos (en el peor de los casos) sólo se verá por otros en el grupo. La red corporativa o de área amplia es un ejemplo de una red privada. La línea entre una red privada y pública siempre se ha trazado en el router del gateway, donde una compañía pone un firewall para mantener a los agentes externos de la red publica fuera de su red privada, o para librar a sus usuarios internos de estar en la red pública.

Hubo un tiempo, no muy atrás, cuando las compañías permitían que sus LAN funcionaran separadamente, cada oficina regional podría tener su propia LAN, con su propio esquema, sistema de correo electrónico, y aun su propio protocolo favorito de red del cual ninguno podría ser compatible con otros esquemas, sin embargo, a medida que los recursos de las compañía se pasaron a las computadoras, vino una necesidad para que estas oficinas se interconecten. Esto se hizo tradicionalmente usando líneas telefónicas alquiladas de varias velocidades. Usando líneas alquiladas, una compañía puede asegurarse que la conexión esté todo el tiempo disponible. Las líneas telefónicas alquiladas, sin embargo, pueden ser caras. Están típicamente facturadas basándose en una retribución mensual, y gastos de kilometraje. Si una compañía tiene oficinas a campo traviesa, este costo puede ser prohibitivo.

Este capítulo se trata de Red Privada Virtual (VPN), un concepto que nubla la línea entre una red pública y privada. Las VPN le permiten crear una red segura y privada sobre una red pública como Internet, pueden ser creadas usando software, hardware, o una combinación de los dos que crean un enlace seguro entre iguales en una red pública, esto está hecho a través de encriptación, autenticación, túnel, y firewalls.

11.1.1. Que es una vpn.

Una Red Privada Virtual (VPN) es una red de información privada que hace uso de una infraestructura pública de telecomunicaciones, que conecta diferentes segmentos de red o usuarios a una red principal, manteniendo la privacidad a través del uso de un protocolo de túnel o aislamiento así como de otras tecnologías que proveen seguridad. La función principal de una VPN es la de brindar conectividad a una red, a través de una red pública, brindando la integridad de la información.

11.1.2. Porque usar las vpn.

Cuando se implementa una VPN, hay cuatro aspectos fundamentales que deben ser considerados: costo, desempeño, confianza y seguridad. De estas cuatro características, la seguridad es el elemento fundamental ya que sin ésta los otros elementos pueden ser inútiles; no importa qué tan barata, rápida y confiable sea una red, sin la seguridad adecuada, los riesgos pesarán más que los beneficios. Una compañía puede usar Internet para enviar archivos a otras corporaciones; sin embargo, sin medidas y políticas de seguridad adecuadas, la información queda expuesta a ataques.

En lugar de conectarse directamente a la red de la empresa usando una tecnología de red telefónica conmutada(Public Switched Telephone Network), los usuarios de acceso VPN sólo necesitan usar al PSTN para conectarse al punto de presencia local (Point Of Presence) del ISP. El ISP luego usa Internet para remitir a los usuarios del POP a la red del cliente de la empresa. Reenviar la llamada de un usuario por la red provee ahorro de costos dramáticos para el cliente de la empresa.

Mientras los ahorros y la gerencia simplificada son beneficios importantes para las VPN, sólo se puede ganar ventajas competitivas, si se puede garantizar la seguridad de la información transmitida por la red. Hoy, la actividad empresarial en línea no es limitada a insignificante comunicación y acceso a documentos relativamente públicos. Hoy todo se está haciendo en línea. Se accede a los registros del cliente,

las propuestas de ventas, y los contratos corporativos. Se transmite especificaciones del producto, órdenes de compra y documentos legales. Se está negociando y desarrollando productos en línea.

Con los accesos remotos seguros, las conexiones vía modem telefónico pueden transferir datos seguros vía un proveedor de servicios Internet o vía una red corporativa. Los datos se encriptan en el cliente antes de que sean transmitidos y se desencriptan en el firewall. El software proporcionado, habilita a los usuarios remotos a que se puedan conectar a la red corporativa como si estuvieran detrás del firewall. La tecnología de VPN proporciona un medio para usar el canal público de Internet como un canal apropiado para comunicar los datos privados. Con la tecnología de encriptación y encapsulamiento, una VPN básica, crea un pasillo privado a través de Internet, instalando VPNs, se consigue reducir las responsabilidades de gestión de una red local.

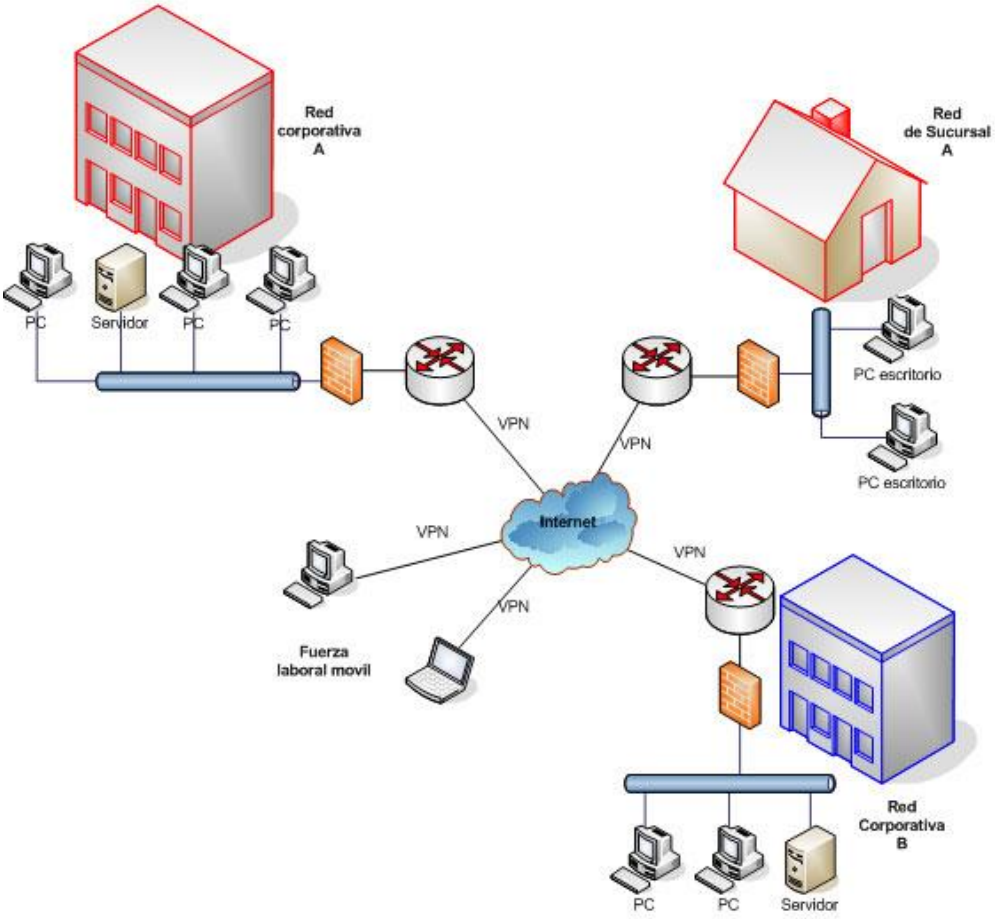


Figura 11.1. Esquema general de las VPN.

11.2. COMO LAS VPN RESUELVEN PROBLEMAS DE SEGURIDAD EN INTERNET.

Una red privada virtual es una red donde todos los usuarios parecen estar en el mismo segmento de red, pero en realidad están en diferentes redes (generalmente públicas) a mucha distancia. Para lograr esta funcionalidad, la tecnología de redes seguras, privadas y virtuales deben completar tres tareas. Primero, deben poder pasar paquetes IP a través de un túnel en la red pública, de manera que dos segmentos de LAN remotos no parezcan estar separados por una red pública. Segundo, la solución debe agregar encriptación, tal que el tráfico que cruce por la red pública no pueda ser espiado, interceptado, leído o modificado. Finalmente, la solución tiene que ser capaz de autenticar positivamente cualquier extremo del enlace de comunicación de manera que un adversario no pueda acceder a los recursos del sistema.

Hay varias tecnologías que las VPN usan para proteger datos que viajan a través de Internet. Los conceptos más importantes son:

- **Firewalls.**
- **Autenticación.**
- **Encriptación.**
- **Túnel.**

11.3. VENTAJAS DE LAS VPN.

Ventajas

- **Seguridad:** provee encriptación y encapsulación de datos de manera que hace que estos viajen codificados y a través de un túnel.
- **Costos:** ahorran grandes sumas de dinero en líneas dedicadas o enlaces físicos.

- **Mejor administración:** cada usuario que se conecta puede tener un numero de IP fijo asignado por el administrador, lo que facilita algunas tareas como por ejemplo mandar impresiones remotamente, aunque también es posible asignar las direcciones IP dinámicamente si así se requiere.
- **Facilidad:** para los usuarios con poca experiencia para conectarse a grandes redes corporativas transfiriendo sus datos de forma segura.

Dentro de las ventajas más significativas se pueden mencionar:

- La integridad, confidencialidad y seguridad de los datos.
- Reducción de costos.
- Sencilla de usar.
- Sencilla instalación del cliente en cualquier PC.
- Control de Acceso basado en políticas de la organización
- Herramientas de diagnostico remoto.
- Los algoritmos de compresión optimizan el tráfico del cliente.
- Evita el alto costo de las actualizaciones y mantenimiento a las PC´s remotas.

Mantener líneas dedicadas para establecer conectividad de acceso remoto aumenta progresivamente cuando la organización crece. Los gastos recurrentes de llamadas de larga distancia hechas por empleados móviles aumentan costos de comunicación. Un número de empleados prefiere trabajar en casa por razones diferentes. Tales empleados requieren acceso a los recursos en la oficina corporativa. Una VPN provee los requisitos de acceso remotos de estos empleados. Una VPN provee los siguientes beneficios:

- El costo de establecer y mantener una VPN es más bajo del costo de un modelo remoto tradicional de acceso. La responsabilidad de implementar y mantener la VPN puede ser pasada al ISP.
- Una VPN le permite a los usuarios remotos fácilmente conectarse a una LAN corporativa a través de una conexión VPN, un gran número de POP le permite

a los usuarios remotos dial-up a un ISP y establecer conexiones VPN de diversas posiciones.

- Una VPN provee mayor flexibilidad cuándo se compara a un modelo de acceso remoto tradicional. Es más fácil de establecer. También se puede modificar una VPN para incorporar los requisitos cambiantes del sistema de redes de una organización. Por ejemplo, en una VPN, para conectar a dos oficinas regionales nuevas con la oficina corporativa, se necesita instalar una conexión telefónica local y un modem para conectarse al POP local de un ISP, es más difícil que establecer una conexión remota de acceso por líneas rentadas permanentes utilizadas en el modelo remoto tradicional de acceso.
- Un número de autenticación sofisticada y esquemas de encriptación, como contraseñas, certificados digitales, y algoritmos de encriptación, sirve para asegurar los datos enviados sobre una VPN. Se puede asegurar la seguridad de la red privada en la oficina corporativa permitiéndole a usuarios remotos acceder sólo recursos específicos. Los niveles diferentes de acceso remoto están definidos para usuarios remotos diversos.
- Una ventaja principal de usar una VPN es el costo bajo de comunicación de acceso remoto. Un VPN no sólo salva el costo recurrente de llamadas de larga distancia sino que también salva el costo de líneas dedicadas rentadas. Además, sólo los cargos locales de llamada son obtenidos para establecer una conexión VPN entre usuarios móviles y la intranet corporativa.

11.4. COMPONENTES DE UNA VPN

Este capítulo enfoca la atención en las tecnologías de fondo usadas para construir una VPN, hay dos campos competentes en el trabajo cuando se habla de conectar redes. El primer campo coloca en el valor más alto la accesibilidad a los datos de dondequiera que el usuario podría estar, y dondequiera que los datos podrían estar. El segundo hace énfasis en la protección de los datos mismos, el contenido, es más importante y debe ser protegido para impedirle a personas no autorizadas usarla. Como se puede ver, estos dos conceptos no están en todo mutuamente exclusivo. Como se enfoca la atención en compartir más y más información a fin de que todo el

mundo pueda obtener lo que necesitan, también se debe permanecer canalizado a la seguridad de esa información a fin de que los demás no se aprovechen.

Porque Internet es una colección vasta de recursos, esta claro que compartiendo la información con otros participantes, pueda ayudar a prosperar. No es claro, sin embargo, a qué riesgo se somete cuando se conecta. Algunas compañías ven las redes como un mercado inexplotado y enorme, llenas de consumidores y de oportunidades publicitarias, pero no se dan cuenta que Internet tiene su propia versión de un "bajo mundo", esto es, sobre todo, lo que nos obliga a proteger los datos, y dónde el surgimiento de las redes privadas virtuales son un punto de apoyo en el siglo 21. La protección de datos privados es el corazón de la red privada virtual, y las dos tecnologías (encriptación y firewalls) más pertinentes son la que hacen todo esto posible.

11.4.1. Manejo de direcciones.

La solución le debe asignar a un cliente VPN una dirección en la intranet y debe asegurar que las direcciones usadas en ella se mantienen privadas. También, una cierta información necesita ser provista para permitirle al cliente acceder a recursos en la red protegida.

11.4.2. Manejo de llaves.

Para usar encriptación, la solución VPN necesita proveer alguna clase de mecanismo de encriptación de llaves para crear la sesión de túnel.

11.4.3. Firewall

La primera parte de las tecnologías relacionadas con la seguridad es el firewall. Un firewall es un sistema que está en medio de una red interna y el mundo externo.

11.4.4. Protocolos

El túnel es el corazón de la tecnología VPN. Mientras que el costo efectivo de VPN es atribuido al uso de Internet, la confianza y la seguridad que las VPN ofrecen son el resultado directo del túnel.

11.5. ESQUEMAS DE VPN.

11.5.1. VPN de Acceso Remoto.

Como el nombre sugiere, las VPN de acceso Remoto proveen en cualquier momento acceso remoto, móvil, a los empleados a distancia de una organización hacia la red de recursos. Típicamente, estas peticiones remotas de acceso son emitidas por usuarios que están constantemente en movimiento o por sucursales pequeñas y remotas que carecen de una conexión permanente a la red corporativa.

Las VPN de acceso remoto son también llamadas VPN de Usuario a LAN. que se puede usar para unir la mano de obra móvil de una organización con una LAN corporativa sobre Internet.

El servidor VPN tramita peticiones de usuarios remotos y sirve como un gateway de acceso entre la red de área local corporativa e Internet. Todo tráfico VPN entrante y saliente debe ser dirigido a través del servidor VPN para asegurar la seguridad de datos. El servidor VPN y el cliente VPN localizado en los puntos finales de la conexión VPN sacan los datos haciendo un túnel, encriptando, y haciendo procedimientos de autenticación. Como una conexión punto a punto, un túnel seguro se extiende del cliente VPN al servidor VPN. Este tipo de túnel es llamado túnel “Unido por los Extremos”.

Hay muchas ventajas ofrecidas por una VPN de Acceso Remoto sobre una Red de Área Amplia de Acceso Dial-UP tradicional.
En una Red de Área Amplia a través de Acceso Dial-Up tradicional, un usuario remoto hace una llamada de larga distancia para establecer una conexión con la red de área local corporativa. La organización obtiene estos cargos de larga distancia de llamada, los cuáles son directamente proporcionales al número de usuarios remotos.

En una VPN de Acceso Remoto, sin embargo, la tarea de establecer y mantener la VPN puede ser pasada a un ISP.

En una VPN de Acceso Remoto, el uso de un POP local de un ISP asegura que sólo los cargos locales de llamada sean obtenidos. Como consecuencia, los costos de comunicación son inferiores comparados con un modelo de Acceso Dial-UP tradicional.

El uso de VPN de Acceso Remoto dará como resultado costos inferiores de comunicación sólo si un usuario remoto tiene que hacer una llamada de larga distancia para acceder a la red de área local corporativa. De otra manera, una conexión establecida usando el modelo de Acceso Dial-Up tradicional es una mejor alternativa.

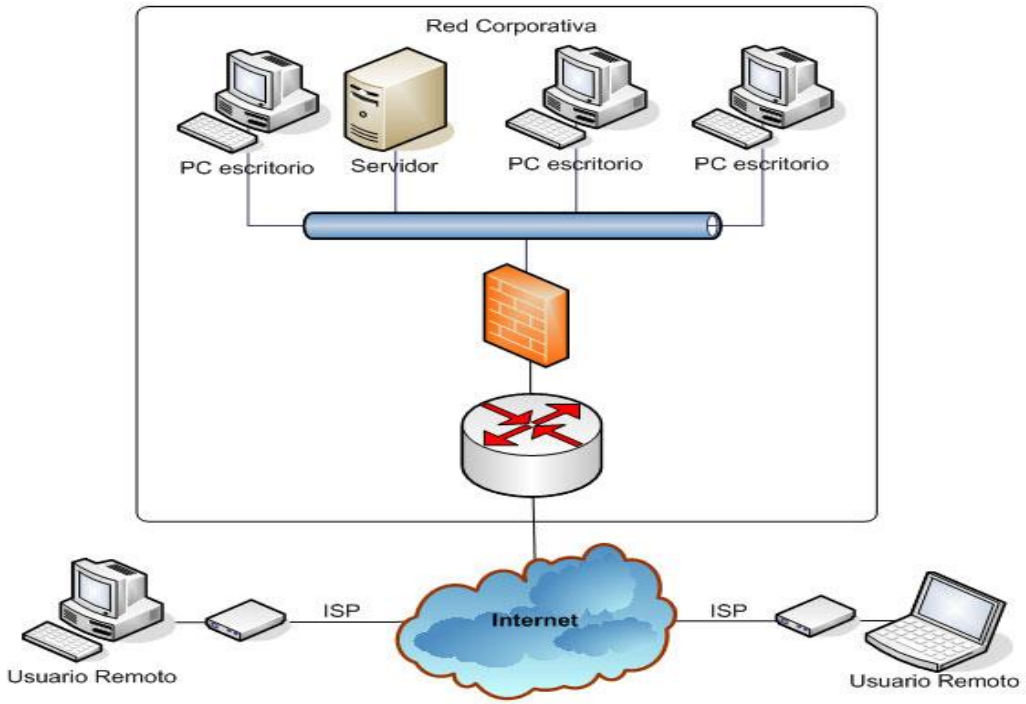


Figura 11.2. VPN de acceso remoto

Para Implementar una VPN de Acceso Remoto, los usuarios remotos y oficinas regionales sólo necesitan establecer conexiones dial-up locales hacia el ISP o POP y conectarse a la red corporativa a través de Internet.

La mayor ventaja de las VPN de acceso, sobre el acceso remoto tradicional es la siguiente:

La necesidad de un RAS y su depósito de módem asociado es completamente eliminada.

- La necesidad de personal de soporte es eliminada porque la conectividad remota es facilitada por el procesador de grupos de instrucciones.
- La necesidad de conexiones con dial a gran distancia es eliminada; en lugar de eso, las conexiones de gran distancia son reemplazadas por conexiones dial-up local.
- La provisión del servicio dial-up barato para usuarios a gran distancia.
- Porque el dial-up de acceso es local, los módems funcionan en tasas superiores de datos comparados al acceso de gran distancia.

- Las VPN le proveen la mejor accesibilidad al sitio corporativo porque soportan un nivel mínimo de servicios de acceso a pesar del incremento en el número de usuarios simultáneos accediendo a la red. Como el número de usuarios conectados aumenta en un esquema VPN, aunque los servicios pueden ser disminuidos, la accesibilidad no es completamente desordenada.

A pesar del número de ventajas ofrecidas por las VPN de acceso remoto, algunas desventajas inherentes son asociadas a ellas. Estas incluyen lo siguiente:

- Las VPN de Acceso Remoto no ofrecen un QoS garantizado.
- La posibilidad de pérdida de datos está por las nubes. Además, los paquetes pueden ser entregados fragmentados y fuera de orden.
- Por la complejidad de los algoritmos de encriptación, el encabezado del protocolo es aumentado considerablemente. Esto conduce a la latencia en el proceso de autenticación. Además, compresión de datos basada en IP y PPP es sumamente lento.
- Por la presencia fundamental de Internet, al transmitir datos multimedia superiores a través de los túneles VPN de acceso remoto, la latencia en la transmisión puede estar por las nubes y el rendimiento específico puede ser sumamente bajo.

11.5.2. VPN Sitio a Sitio

Las VPN Router a Router son también llamadas VPN LAN a LAN porque se usa para conectar dos o más redes privadas. Se puede usar una VPN Router a Router para establecer una conexión remota de acceso entre la red de área local corporativa de una compañía y la red de área local en una oficina regional o la oficina de un socio comercial. Funciona en cierto modo parecido a un enlace de Red de Area Amplia entre dos sitios remotos.

Hay dos tipos de VPNs Router a Router, Sitio a sitio (Site to Site) basado en intranet y Sitio a sitio (Site to Site) basado en extranet.

a. VPN Sitio a Sitio basada en intranet.

VPN Sitio a Sitio basado en intranet conecta dos o más redes privadas dentro de una organización sobre un armazón de Internet. Se puede usar una VPN sitio a sitio basado en intranets para crear un medio seguro de comunicación entre una oficina corporativa y oficinas regionales de una organización.

Esta VPN provee la solución ideal para una organización que necesita conectar un número de oficinas regionales remotas con la oficina corporativa. Por ejemplo, XYZ S.A. es una corporación multinacional que consta de una cadena restaurantes de comida rápida, la oficina corporativa está ubicada en Nueva York y las oficinas regionales son localizadas en Los Ángeles, San Francisco, Melbourne, Madrid, París, y Munich. Para conectar la red de área local de la oficina regional en Madrid con la red de área local en la oficina corporativa en Nueva York, se necesita establecer una VPN Sitio a Sitio basado en intranet. Esta VPN es configurada usando conectividad a través de países diversos, las líneas dedicadas rentadas se usan para conectar LANs a un procesador de grupos de instrucciones.

Lo dos servidores VPN localizados en los puntos finales de la conexión VPN actúan como enrutadores y controlan el flujo de tráfico de datos sobre el VPN. Un servidor VPN actúa como una puerta de enlace entre la red de área local en la oficina regional y la Internet. El servidor VPN en el otro extremo de la conexión VPN tramita las peticiones de conexión, y entonces redirige esas peticiones a la red de área local corporativa. En este tipo de VPN, el túnel se extiende del borde de una red de área local al borde del otro. Este tipo de túnel es llamado Túnel Nodo a Nodo.

Las líneas dedicadas son usadas sólo para conectar la red de área local a un POP local de un ISP. Como consecuencia, los costos de comunicación son muy inferiores comparado con un modelo tradicional de Red de Área Amplia.

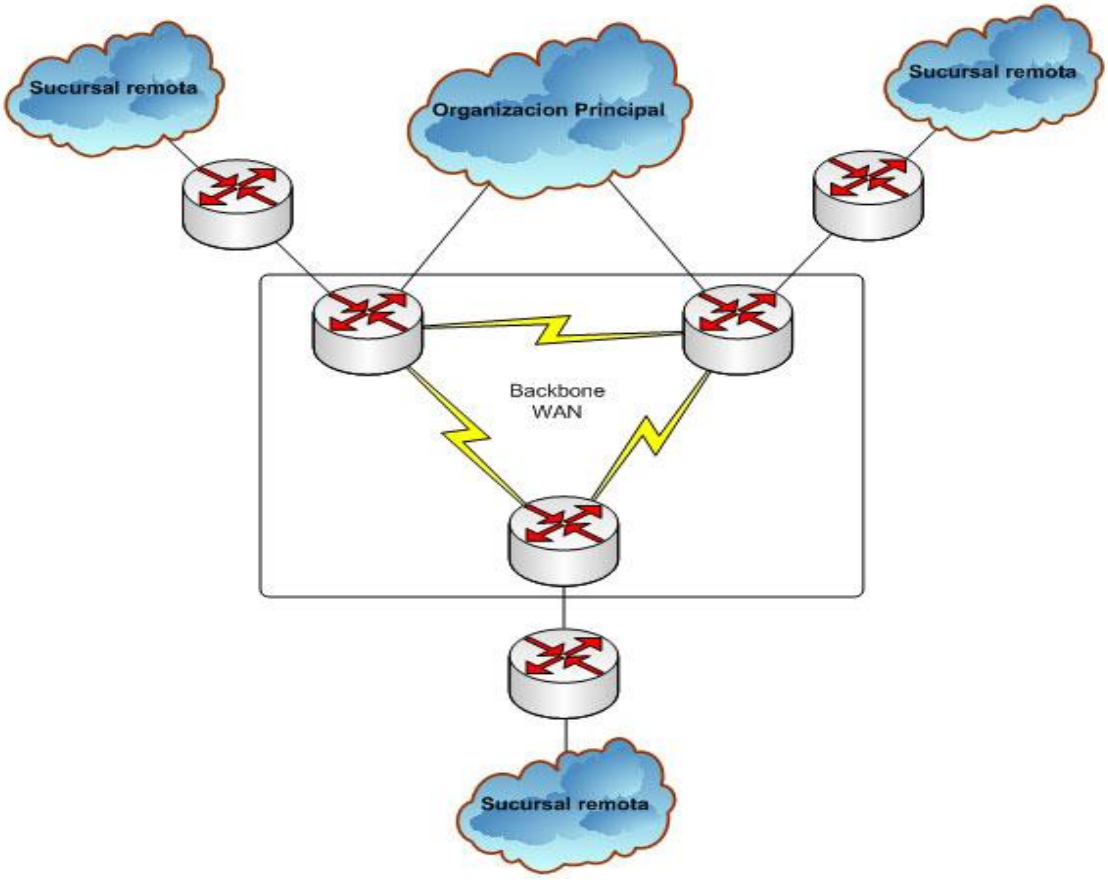


Figura 11.3. El esquema de la intranet usando WAN backbone.

Este esquema es altamente caro porque al menos dos routers están obligados a conectar un campus remoto a la red de la organización. Además, la implementación, el mantenimiento, y manejo del backbone de la red pueden ser sumamente caros a merced del volumen de tráfico de la red que lo atraviesa y la extensión geográfica de la intranet entera. ¡Por ejemplo, el costo de una intranet global puede ascender hasta muchos miles de dólares al mes! Mientras mayor el alcance de la intranet, más caro puede ser.

Con la implementación de soluciones VPN, el costo del backbone de WAN es reemplazada por el bajo costo de la conectividad a Internet, lo que puede disminuir el costo total de la implementación de la intranet completa.

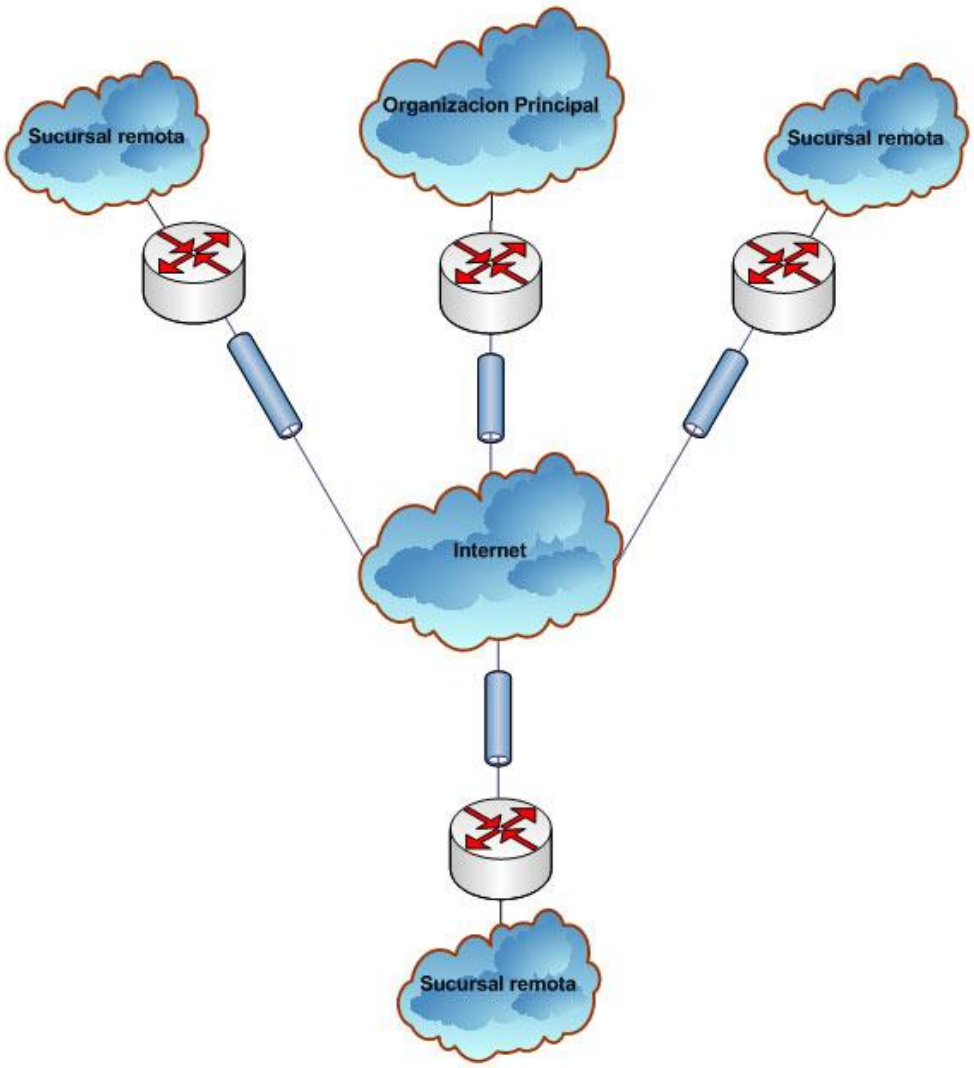


Figura 11.4. Esquema VPN basado en intranet.

Las mayores ventajas ofrecidas por este esquema son las siguientes:

- Es eficiente en base a costos debido a la eliminación de routers que se usan para formar el backbone WAN.
- Considerablemente reduce el número de personal requerido para soporte a través del globo, situados en sitios remotos diversos.
- Porque Internet actúa como el médium de conexión, es más fácil acomodar enlaces punto a punto.

- Facilidad de respaldo y eficiente en base a costos en los que puede ser usados los túnel de VPN en colaboración con la tecnología de conmutación rápida, como Frame Relay.
- Por la naturaleza local de dial-up la conectividad al ISP y la accesibilidad es más acelerada y mejor. También, la eliminación de servicios a gran distancia ayuda a un organismo a reducir el costo de operación de la intranet.

Las desventajas asociadas con soluciones de la intranet VPN se encuentran enumeradas como sigue:

- Porque los datos son todavía enviados a través de un túnel en una red pública compartida, un ataque DoS, todavía puede plantear amenazas de seguridad serias.
- La posibilidad de pérdida de paquetes de datos mientras se transmiten está todavía muy alta.
- En caso de transmisión de datos superiores, como multimedios, la latencia en la transmisión puede estar muy alta y el rendimiento específico puede ser sumamente bajo debido a la presencia básica de Internet.
- Por la conectividad fundamental a Internet, el desempeño puede ser esporádico y QoS no puede ser garantizado.

b. VPN Sitio a Sitio basado en extranets.

VPN sitio a sitio basado en extranets son usadas para conectar las redes privadas de dos o más organizaciones. Una VPN basada en extranet provee un medio seguro para compartir información y aplicaciones en un protocolo basado en IP. Se puede usar esta VPN para crear un ambiente compartido seguro entre una organización y una entidad externa, como un cliente o un socio comercial. Esta VPN le permite proveer un nuevo valor agregado a los servicios de las entidades externas, estas entidades externas son libres de acceder recursos limitados dependiendo de sus requisitos, como consecuencia, eficazmente se puede coordinar con clientes, proveedores, socios comerciales, y agencias de subcontratación.

Una compañía “A” esta localizada en Los Ángeles que comercia material de presas y equipo. La “B”., localizada en Manila, es uno de los proveedores principales de “A”. Los empleados de “B” frecuentemente requieren acceder a la información de compras y el departamento de cuentas de “A”, continuando con las órdenes y los pagos, se puede usar una VPN Sitio a Sitio basado en extranet en esta situación para conectar las redes privadas de las dos compañías. “A” puede usar esta VPN para permitir a los empleados de “B” el acceso limitado a la información en la compra y el departamento de cuentas.

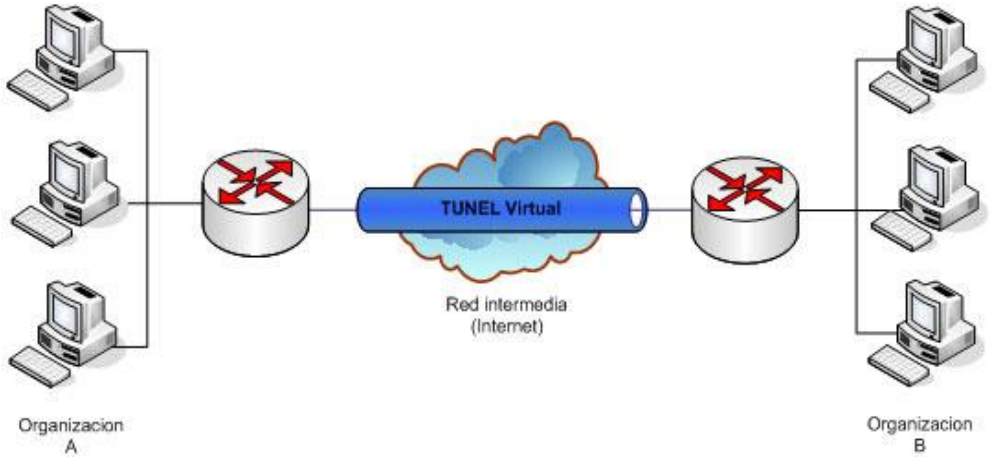


Figura 11.5. VPN Sitio a Sitio basado en extranets.

Tal como en el caso de una VPN Sitio a Sitio basado en intranet, los servidores VPN localizados en los puntos finales de la conexión VPN controlan el flujo de tráfico de datos. El método de túnel nodo a nodo es usado en esta VPN, y el túnel se extiende del borde de una red de área local a la otra red de área local.

En esta VPN, la petición de conexión de un usuario es redirigida al servidor VPN, lo cual establece una conexión segura con el servidor VPN en un sitio remoto. El servidor VPN tramita la petición antes de reenviarla a la LAN corporativa. Las líneas dedicadas son usadas sólo para conectarse a un POP local de un ISP.

El esquema tradicional es sumamente caro, porque cada red separada en la intranet debe estar hecha a la medida según la red externa. Esto típicamente da como

resultado administración e implementación complicada, la necesidad de personal capacitado para mantenimiento y manejo de este esquema sumamente complicado es muy alta. Además, este tipo de esquema no puede ser fácilmente extendido porque de hacerlo así desordenaría la intranet entera y podría afectar las otras redes externas conectadas. Toda implementación de extranets puede ser la pesadilla de un diseñador de red y de un administrador.

Las mayores ventajas de las Extranet VPN incluyen lo siguiente:

- El costo fraccionado se compara al esquema tradicional.
- La fácil implementación, el mantenimiento, y la facilidad de modificación del esquema existente.
- Por la presencia fundamental de Internet, se tiene una mayor elección de vendedores cuándo hacen y miden soluciones según las necesidades de una organización.
- Porque la parte de conectividad de Internet es mantenida por el ISP, la necesidad de personal para soporte se acorta considerablemente, así descendiendo el costo de operación del esquema entero.

Algunas desventajas asociadas con la solución Extranet VPN incluyen lo siguiente:

- Las amenazas de seguridad, como DoS, todavía existen.
- El riesgo de violación de la intranet de la organización ha aumentado.
- Debido a la presencia fundamental de Internet, en caso de datos superiores, como multimedios, la latencia en la transmisión puede ser muy alta y el rendimiento específico puede ser sumamente bajo.
- Por la conectividad de Internet fundamental, la actuación puede ser esporádica y QoS no puede ser garantizado.

Los requisitos de conectividad de acceso remoto de las organizaciones varia dependiendo del tipo de la organización y la composición de su fuerza laboral. Algunas organizaciones tienen a un gran número de usuarios móviles. Los otros tienen un número de oficinas regionales difundidas a través de posiciones

geográficas diferentes. Una organización debe considerar estos requisitos antes de seleccionar un tipo particular de Red Privada Virtual (VPN).

11.5.3. Las VPN Voice/IP Mejoradas

Las VPNs VoiceIP mejoradas soportan telefonía segura de Internet. Es parecido a una Intranet VPN pero, en lugar de hacer un túnel a través de la encriptación de datos, se encripta la voz en un túnel a través de Internet.

11.5.4. Las VPN Corporativas

Las VPN Corporativas se usan para soportar la convergencia de las aplicaciones de voz y de datos eficazmente sobre Internet. Combinan VPN de datos (generalmente solo Intranet VPN) con VPN Voice.

11.6. TIPOS ESPECIALES DE VPN.

Además de los dos tipos genéricos de VPN, dos tipos especiales de VPN han estado definidos para conectividad remota abastecedora de acceso. Estos tipos especiales de VPN estaban definidos no sólo a responsabilizarse por cambiar los requisitos comerciales, sino que también a vencer algunas limitaciones de las VPN anteriores.

11.6.1. VPN Pass-Through.

Una VPN Pass-Through combina las características de una VPN Sitio a Sitio basado en intranet y Sitio a Sitio basada en extranet. Este VPN le permite a un usuario remoto acceder a la intranet de una compañía para conectarse a Internet. Una conexión VPN es luego provista con la intranet de otra compañía con la cual se encuentra en red. Los empleados móviles usan esta VPN para acceder a los recursos corporativos usando la intranet corporativa de alguna otra organización.

Por ejemplo, Tom Jones, un empleado de una Organización, está en una visita comercial a la oficina corporativa de un cliente en Chicago. Tom necesita acceder a alguna información de la oficina corporativa en Nueva York. Una VPN Pass-Through provee una solución factible en esta situación.

Tom realiza los siguientes pasos para establecer una conexión VPN Pass-Through:

1. Usa una laptop para establecer una conexión segura con el servidor VPN de la intranet del cliente. Un túnel seguro es creado entre el servidor VPN y la laptop de Tom.
2. Marca a un POP local de un ISP para conectarse a Internet.
3. Usa el software del cliente VPN en su laptop para establecer una conexión VPN con el servidor VPN, en segundo lugar el túnel seguro es creado, que se extiende de la computadora portátil de Tom a través de la intranet corporativa del cliente y la Internet al servidor VPN de . la Organización B.

El segundo túnel es creado dentro del primer túnel en una VPN Pass-Through, después de que la conexión VPN es establecida, Tom puede acceder a los recursos en la intranet corporativa de la organización B.

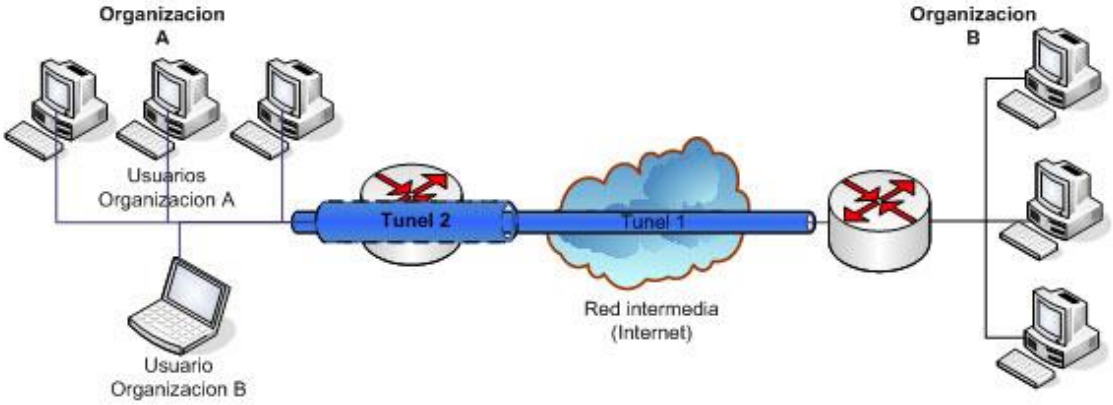


Figura 11.6. VPN Pass-Through

11.6.2. VPN basadas en MPLS.

MPLS es una técnica que fomenta el uso de datos para mejorar el cambio de paquetes basados en protocolos IP a través de una red. Combina la capacidad

conmutada del nivel de enlace de datos y la capacidad de enrutamiento del nivel de red en el modelo de interconexión de sistemas abiertos.

MPLS involucra la adición de una etiqueta a un paquete entrante de datos, la cual contiene información de ruteo, algo semejante como la dirección de destino, un número que identifica la VPN, y la ruta que va usar el paquete. Los enrutadores dentro de una red necesitan examinar la información en la etiqueta de un paquete entrante de datos para enviarlo a través de la red. En el otro extremo de la red, un enrutador remueve la etiqueta del paquete de datos antes de remitirle su destino final. MPLS ayuda a limitar el procesamiento de paquetes de datos en los extremos de una red. La remoción de procesamiento intermedio provee mayor dimensionalidad de la red y eficiencia superior comparables a redes basadas en protocolos IP. Un ISP usa una red MPLS para proveer calidad de servicio (Quality Of Service), y una solución escalable de sistema de redes a los clientes.

Los componentes de una red MPLS son:

- Routers comutador de etiquetas del perímetro (ELSR, Edge Label Switch Router): Localizados al borde de la red de ISP, estos son también llamados enrutadores de perimetro del proveedor (PE, Provider Edge). Un router conmutador de etiquetas del borde está conectado con múltiples enrutadores del borde del cliente (CE, Client Edge). La tarea de sumar y remover etiquetas de paquetes de datos es llevada a cabo por estos enrutadores. Los enrutadores localizados en los POP de un ISP representan router conmutadores de etiqueta del borde.
- Router de conmutación de etiquetas (LSR, Label Switch Router): localizado en el corazón de una red basada en MPLS de un ISP. También llamados enrutadores del proveedor, estos enrutadores cambian los paquetes etiquetados basandose en la información contenida en las etiquetas, los enrutadores dentro de la red de ISP representan LSR.
- Enrutadores de extremo del cliente (CER, Customer Edge Router) : Localizados en el sitio del cliente, los enrutadores en una oficina corporativa,

una oficina regional, o la oficina de un socio comercial representan enrutadores de extremo.

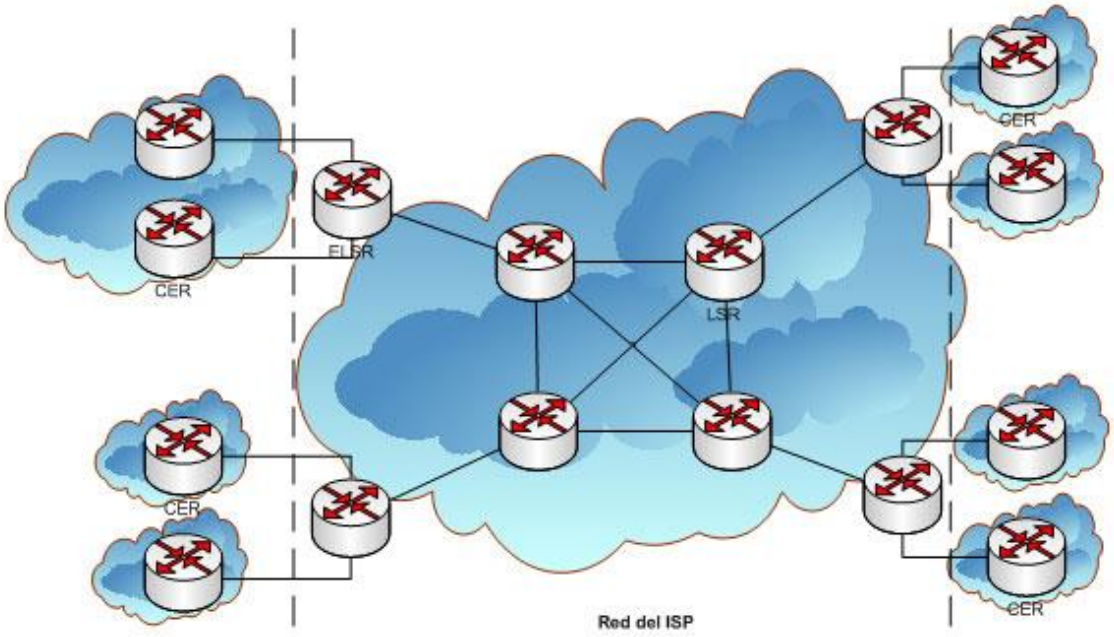


Figura 11.7. VPN MPLS.

Un ISP puede usar tecnología MPLS para proveer los mejores servicios a los clientes. Una red basada en MPLS disminuye el tiempo de tránsito para paquetes de datos a través de la red del ISP. Además, la aplicación de Capa 3, la tecnología MPLS no requiere conexiones punto a punto dentro de los sitios remotos de una VPN. Como consecuencia, un ISP puede proveer la conectividad de acceso remoto a un mayor número de clientes.

11.6.3. VPN MPLS de Capa 2.

La mayoría de ISP alrededor del mundo usan VPN MPLS de capa 2. Esta VPN consta de un número de túneles punto a punto que son establecidos sobre la red del ISP. VPN MPLS de capa 2 usan el modelo de cubierta para establecer una conexión punto a punto entre dos sitios. En el modelo de cubierta, un enrutador en un sitio remoto establece una conexión punto a punto con enrutadores en los otros sitios, si una organización consta de una oficina corporativa y cinco ramas, se necesitará establecer un enrutador en cada sitio, además, se tendrá que colocar cinco

conexiones punto a punto entre el enrutador en la oficina corporativa y los enrutadores en las oficinas regionales.

La información de enrutamiento es controlada por el cliente y no por el ISP. Este modelo usa Interior Gateway Protocol (IGP) para manejar las tablas de enrutamiento. El Routing Information Protocol (RIP) y Open Shortes Path First (OSPF) son ejemplos de IGP que se usan para manejar enrutamiento dentro de un sistema autónomo.

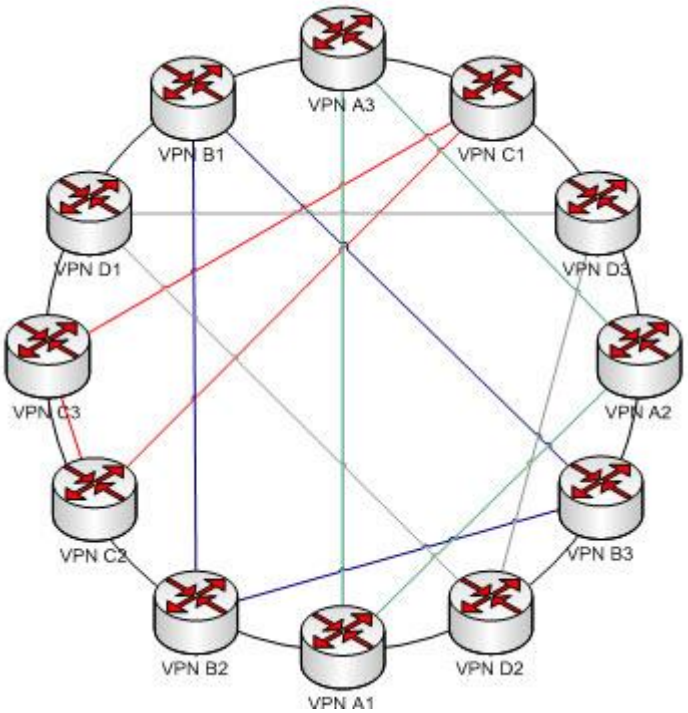


Figura 11.8. VPN MPLS de Capa 2

La figura muestra cuatro VPN interconectadas: A, B, C y D. Estas VPN usan los servicios del mismo ISP. La VPN A consta de tres sitios remotos interconectados: La VPN A1, VPN A2, y VPN A3. Un enrutador separado es utilizado en cada sitio que se conecta con los enrutadores en otros sitios para establecer una conexión punto a punto, por ejemplo, VPN A1 tiene dos conexiones punto a punto , la cuál provee un enlace de la VPN A3 y VPN A2 . Si un sitio nuevo es agregado a la VPN A, se tendrá que establecer un enrutador nuevo en ese sitio y configurar los enrutadores en todos los demás sitios para establecer conexiones punto a punto con el sitio nuevo. Los problemas de dimensionalidad ocurren si una VPN consta de un gran número de

sitios remotos. Además, el gran número de conexiones punto a punto limita la aptitud de un ISP para proveer conectividad de acceso remoto a un número limitado de clientes.

A pesar de los problemas de dimensionalidad, las VPN MPLS de capa 2 son usadas extensamente para proveer conectividad de acceso remoto entre sitios remotos. Una VPN MPLS de Capa 2 es usada en las siguientes situaciones:

- EL ISP actúa sólo como un transportador del portador, además de los controles del cliente y los procedimientos de enrutamiento.
- La estructura de la VPN es simple y consta sólo de algunos sitios remotos.
- El soporte para direcciones IP duplicadas necesita ser incorporado en un VPN.
- La estructura de una VPN es estática y la adición de sitios nuevos no es regularmente requerida.
- El ISP le provee a la VPN de capa 2 servicios orientados de transporte y no pueden manejar el costo de la infraestructura y conmutación en una VPN MPLS de capa 3.

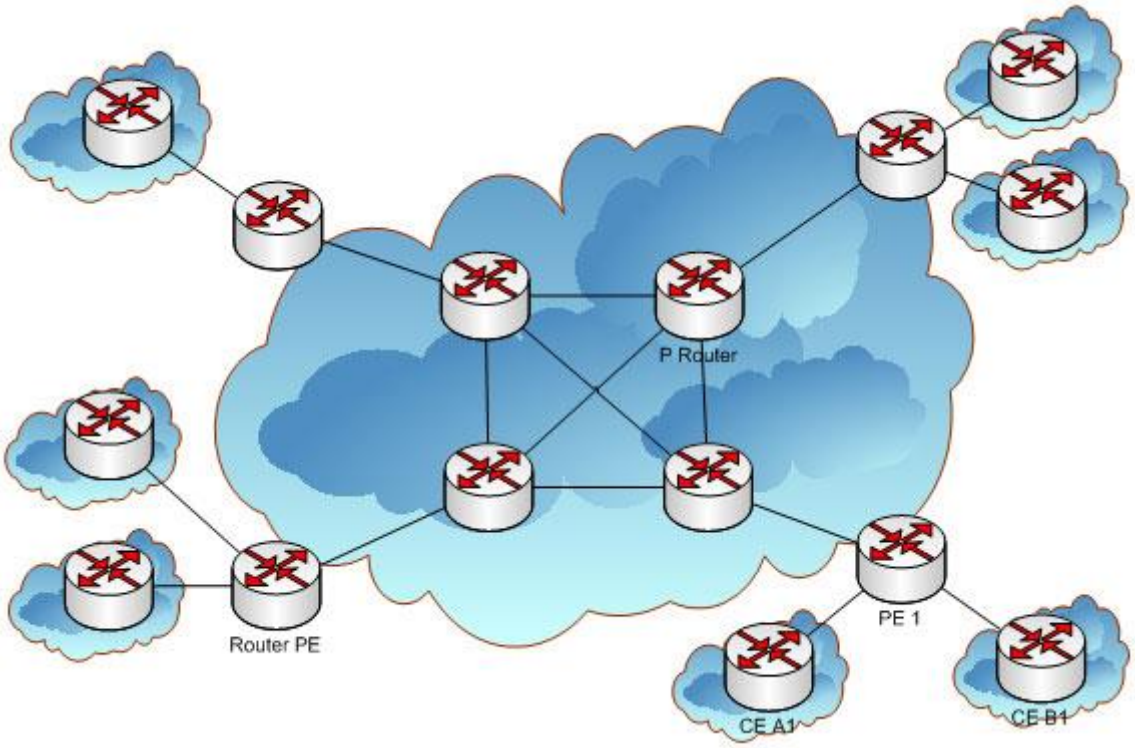
11.6.4. VPN MPLS de capa 3.

Las VPN MPLS de capa 3 fueron desarrolladas para vencer las limitaciones de las VPN MPLS de capa 2. Los modelos peer-to-peer se usan para proveer una solución dimensionable de VPN. En una VPN MPLS de capa 3, un enrutador CE se comunica con sólo un enrutador PE de la red del ISP. El enrutador CE no está obligado a establecer conectividad punto a punto con los enrutadores en diversos sitios remotos. Una conexión peer to peer es establecida entre un enrutador CE y un enrutador PE. El modelo peer to peer usa el Border Gateway Protocol (BGP).

Nota

BGP es extensamente utilizado como un Exterior Gateway Protocol (EGP), es usado para direccional información entre enrutadores que se usan para conectar diversos sistemas autónomos. Un sistema autónomo consta de un número de redes que son

agrupadas conjuntamente para formar una súper red. El esquema de direccionamiento BGP IP le permite simplificar la estructura de tablas de enrutamiento por la combinación de múltiples entradas de ruteo en una sola tabla de ruteo.



VPN

Figura 11.9. VPN MPLS de capa 3

Los enrutadores CE en el sitio del cliente conectan a un enrutador PE en la red del ISP, se puede configurar un enrutador PE para establecer una enlace Peer to Peer con múltiples enrutadores CE de clientes diferentes. Por ejemplo, los enrutadores CE A1 y CE B1 están conectados al enrutador PE y PE1 esta en la red del ISP. Los enrutadores PE actúan como puertas de enlace para la red del ISP ayudando a recibir y redireccionar la información entre los enrutadores que se establecen en los sitios remotos.

Una VPN Routing and Forwarding (VRF) mantiene una tabla en cada enrutador PE para cada sitio conectado a ese enrutador, la tabla VRF almacena información

acerca de las rutas asociadas con una VPN en particular. Un identificador VPN, llamado un blanco de ruta, es asignado a cada ruta VPN para distinguirla de las otras rutas. Este identificador VPN forma una parte de una etiqueta que está pegada a un paquete de datos por el enrutador PE. Los enrutadores PE dentro de la red de ISP usan etiquetas para reenviar paquetes de datos recibidos de enrutadores PE. Nótese que ninguna información de enrutamiento se guarda dentro de enrutadores PE.

Las ventajas de usar una VPN MPLS de Capa 3 son:

- Alta escalabilidad :
    - Provee una opción para facilitar la modificación de la estructura de la VPN.
    - Simplifica el procedimiento para la adición y la remoción de sitios de una VPN existente.
- Arquitectura sin conexión: Le permite a un ISP proveer la conectividad del Internet a un gran número de clientes, esta VPN no requiere que túneles o conexiones virtuales punto a punto sean establecidas entre los sitios de una VPN. Como consecuencia, la tarea de establecer y mantener la VPN se pone mucho más fácil que con una VPN MPLS de Capa 2.
- Seguridad: Provee el mismo nivel de protección comparado con las VPN orientadas a conexión. Los identificadores VPN ayudan a asegurar la integridad de los datos para la prevención de mezcla entre los datos de diferentes VPN.
- Integración libre de irregularidades: Permite fácil implementación de una VPN sin que sea necesario hacer cambios en la red existente del cliente. Un cliente sólo mantiene enrutadores CE que no son necesarios para soportar MPLS.

La desventaja de usar una MPLS de capa 3 es que se requiere un nivel elevado de capacidad de procesamiento para enrutadores PE, múltiples tablas VRF necesitan ser mantenidas en cada enrutador PE. Estas tablas contienen información de ruteo separadas, relacionadas a cada VPN. Además, un enrutador PE le asigna una

etiqueta a cada paquete de datos antes de remitirlos a los enrutadores PE dentro de la red ISP, sólo los enrutadores sofisticados pueden soportar estos requisitos de procesamiento.

No todos los ISP permiten formar una arquitectura para una VPN MPLS de Capa 3. Una VPN MPLS de Capa 3 es apropiada en las siguientes situaciones:

- La VPN consta de un gran número de sitios y que frecuentemente se suman sitios nuevos a la VPN existente.
- El ISP provee servicios a un gran número de clientes y puede recuperarse el costo de establecer y mantener el tránsito basado en MPLS de una red.

11.7. LAS SOLUCIONES VPN.

Un VPN es un conglomerado de tecnologías útiles que originalmente fueron ensambladas a mano. Ahora las compañías que se enlazan a través del ISP se han dado cuenta del valor de una VPN y le ofrecen productos que hacen el trabajo arduo por usted. Además, hay una variedad de software gratis disponible en Internet que puede usarse para crear una VPN. A continuación se consideraran una cierta cantidad en detalle de las soluciones comerciales y libres que actualmente se encuentran disponibles. La que se seleccione para una red corporativa en especifico dependerá de los recursos disponibles para su implementación, las plataformas que se utilizan, la topología de red, el tiempo que se tiene para implementación, la inversión que se desea realizar, y si se desea o no soporte comercial. No se puede cubrir todas las soluciones vpn en esta investigación; las tecnologías cambian demasiado rápido, en lugar de eso, se ofrecen criterios y detalles que se pueden usar en todas las redes y productos VPN.

El kit VPN va desde soluciones de software que se ejecutan o se integran a los sistemas operativos de una red (AltaVista Tunnel o CheckPoint Firewall 1 en Windows NT o Unix), y hardware como routers y firewalls (Cisco y Ascend), hasta soluciones de hardware integradas diseñadas específicamente para funciones VPN

(VPNet y Bay Networks Extranet Switch). Algunos protocolos, como SSH o SSL, obtuvieron popularidad por realizar otras funciones, pero desde entonces se han usado también para VPN. Además de los productos, los ISP también ofrecen servicios VPN a sus clientes.

Las VPN pueden ser implementadas de muchas formas. Por ejemplo, dependiendo en que extremo se implementan los requisitos básicos para una VPN, ya sea en el proveedor de servicio o la organización.

Las VPN dependendiendo del contexto en que se implementan se pueden clasificar de la siguiente manera:

- VPN basado en la arquitectura de implementación.
- VPN basado en Arquitecturas de seguridad.

Nota: El túnel usualmente tiene lugar en el equipo del ISP, Si ambos extremos de la conexión están en el mismo ISP, ese ISP le podría ofrecer un Service Level Agreement (SLA) garantizando una cierta cantidad máxima de latencia y tiempo de buena calidad.

11.8. CLASIFICACIÓN DE VPN BASADO EN LA ARQUITECTURA DE IMPLEMENTACIÓN.

Dependiendo de cuál extremo de comunicación es responsable de implementar la VPN y de cuidar los requisitos de seguridad, las VPN pueden ser clasificadas en tres categorías, las cuales son:

- Las VPN dependientes o Subcontratadas.
- Las VPN independientes o Internas.
- Las VPN híbridas.

11.8.1. Las VPN dependientes o Subcontratadas.

En el caso de las VPN dependientes, el proveedor del servicio es responsable de proveer la solución VPN completa. Por consiguiente, es la responsabilidad del proveedor del servicio implementar la infraestructura de túnel y proveer seguridad y rendimiento al asegurar la manejabilidad del esquema. Como consecuencia, la organización suscriptora queda totalmente excluida en este tipo de implementación de VPN. Por esto, la organización no necesita cambiar su infraestructura existente.

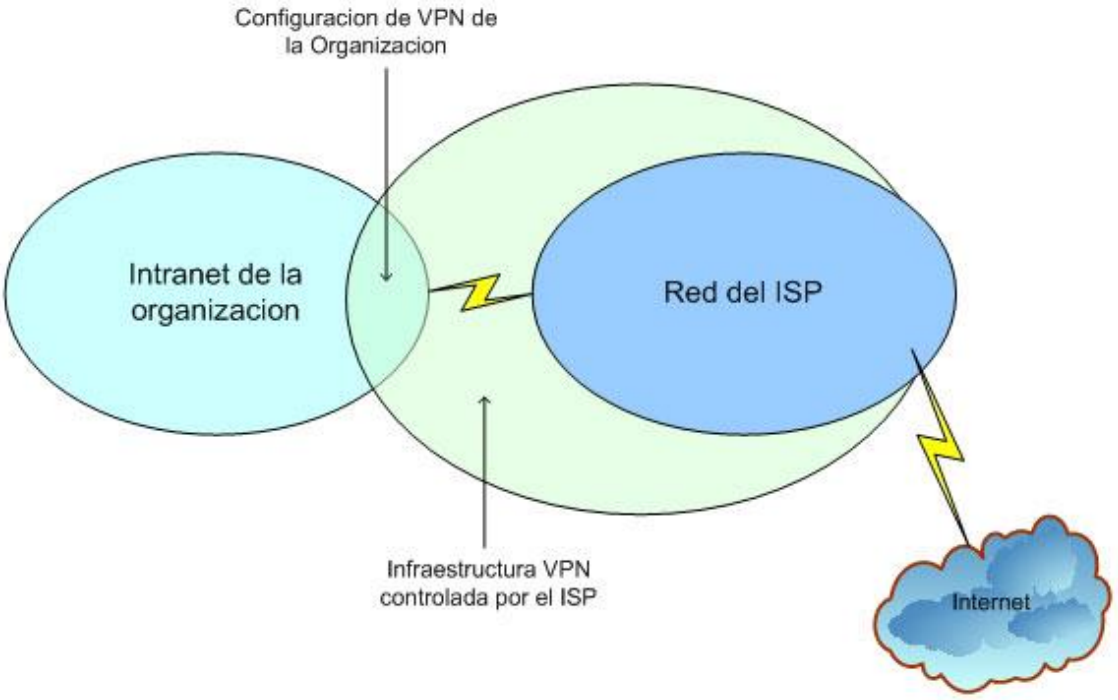


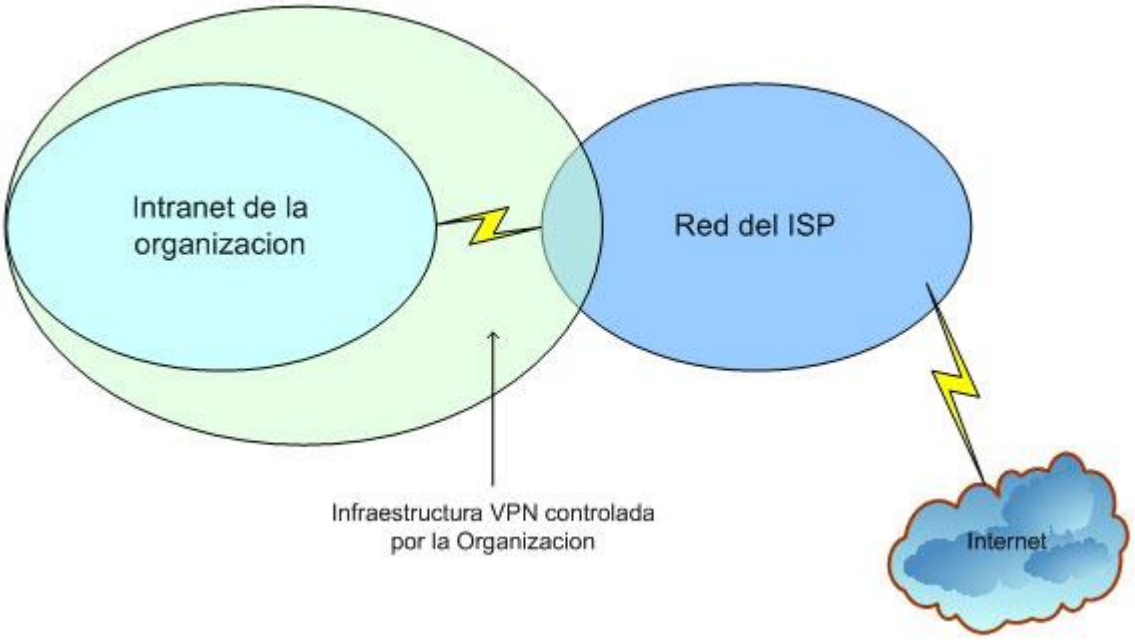
Figura 11.10. La arquitectura VPN dependiente.

Ya que la implementación completa de la VPN y el manejo se hacen por el proveedor de servicio, el proceso de creación del túnel es transparente para los usuarios finales. Cuando un usuario trata de acceder a un recurso remoto o servicio, el Network Access Server (NAS) localizado en el POP del ISP autentica al usuario. Si el NAS almacena la información relacionada con perfiles de los miembros, privilegios y parámetros del túnel, entonces puede autenticar a los usuarios. Sin embargo, el NAS también puede consultar a un servidor RADIUS, AAA, o servidor TACACS para la información requerida. Por consiguiente, ciertas medidas deben ser tomadas por la organización para asegurar la seguridad de sus recursos internos. Como consecuencia, RADIUS, AAA y TACACS no son opcionales en esta arquitectura. Es imprescindible implementar estas medidas de seguridad y preferentemente en la

intranet de la organización, no es cuestión de que tan confiable es el proveedor del servicio.

11.8.2. Las VPN independientes o Internas.

Las VPN independientes son lo contrario de las VPN dependientes. Aquí, la responsabilidad entera de establecer la VPN es manipulada por la organización. El papel del proveedor del servicio en esta arquitectura es insignificante y es relegado para manejar el tráfico de Internet. El túnel y la encriptación/desencriptacion de datos ocurren dentro de la intranet de la organización.



La Figura 11.11. VPN de arquitectura independiente.

Las VPN independientes, ofrecen un nivel alto de seguridad y permiten a la organización mantener el control completo de las transacciones basadas en VPN. La mayoría de administradores consideran que este método es ideal para la seguridad porque la organización no tiene que trasmitir la responsabilidad de la arquitectura VPN a una entidad externa. Además, el coso total de la implementación no es mucho más alto que el costo de VPN dependientes. Sin embargo, este método suma carga adicional relacionada a la administración de red.

11.8.3. Las VPN híbridas.

La arquitectura VPN Híbrida le ofrece una combinación de la arquitectura dependiente e independiente. Este método es usado cuando la organización no subcontrata la solución completa VPN a un proveedor de servicio. En lugar de eso, una parte de la solución VPN es implementada y controlada por la organización mientras el resto es implementado y manejado por el proveedor del servicio.

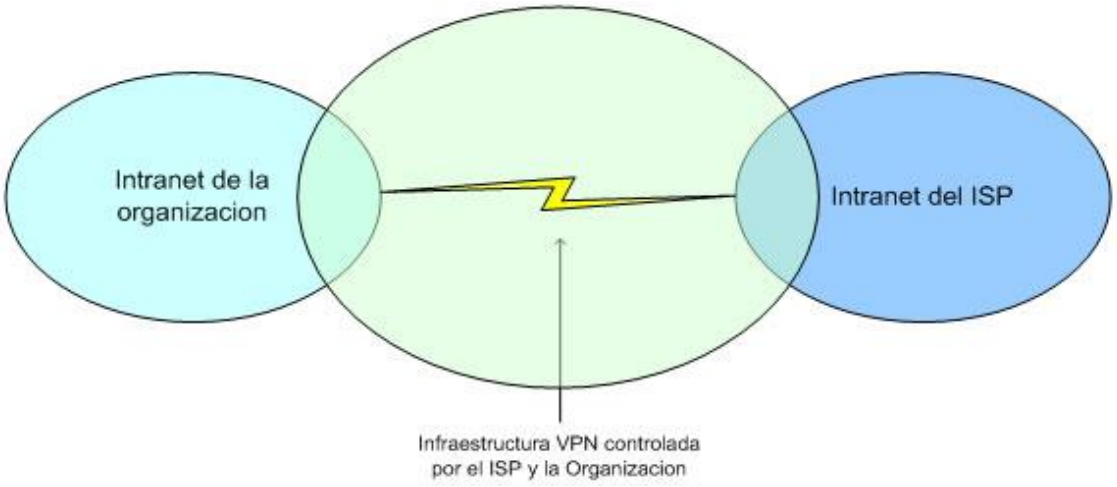


Figura 11.12. La arquitectura VPN híbrida, conjuntamente controlada por la organización y el proveedor de servicio.

Otro modelo para las VPN híbridas, es que la organización subcontrata la solución VPN a múltiples proveedores de servicio en lugar de un solo proveedor controlando el esquema entero como en la arquitectura dependiente. Como consecuencia, ninguno de los proveedores de servicio pueden controlar totalmente la arquitectura y de esta manera, la organización puede implementar una VPN subcontratada sin la carga de administración de la VPN. Sin embargo este método es poco complicado en términos de administración, le permite a la organización eliminar el monopolio de un proveedor de servicio. La ventaja más grande de este método es que establece disponibilidad, si uno de los enlaces de ISP se cae, todavía tiene el otro.

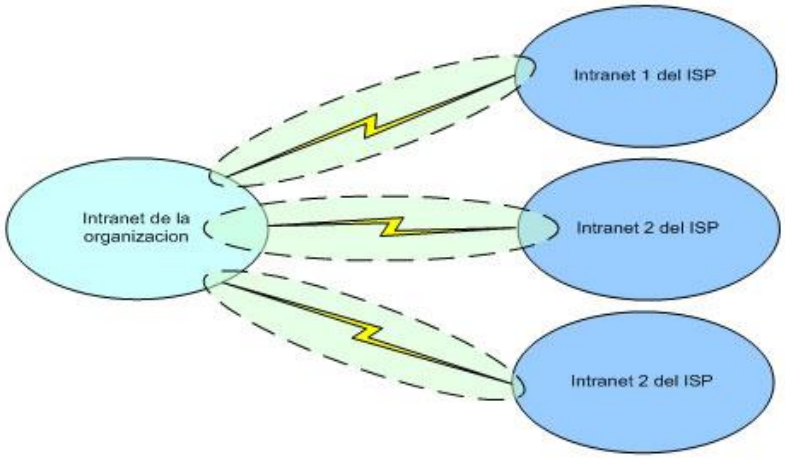


Figura 11.13. La arquitectura VPN híbrida, controlada por múltiples proveedores de servicio.

11.9. VPN BASADO EN ARQUITECTURAS DE SEGURIDAD.

Aunque las VPN son soluciones de seguridad, las siguientes categorías ofrecen a la organización seguridad mejorada:

- Las VPN de Router a Router.
- Las VPN Firewall a Firewall.
- Las VPN Iniciadas por Cliente.
- Las VPN Dirigidas.

11.9.1. Las VPN Router a Router

Las VPN Router a router permiten conectividad segura entre sitios de organizaciones a través del Internet. Las VPN Router a router permiten las siguientes implementaciones:

Túneles de VPN-ON-DEMAND. En esta implementación de VPN, un túnel seguro es establecido entre los routers que están puestos en la conexión al lado del cliente y al lado del servidor. Estos tipos de túneles pueden soportar conexiones múltiples simultáneamente y pueden persistir hasta que la última conexión sea terminada. Para una implementación exitosa de VPN-ON-

DEMAND, los routers en ambos extremos deben soportar capacidades de VPN, como los algoritmos de intercambio de llaves y de encriptación. Una desventaja grande de este modelo es que estos túneles router a router son específicos para el protocolo del proveedor de servicio escogido de la intranet o del túnel.

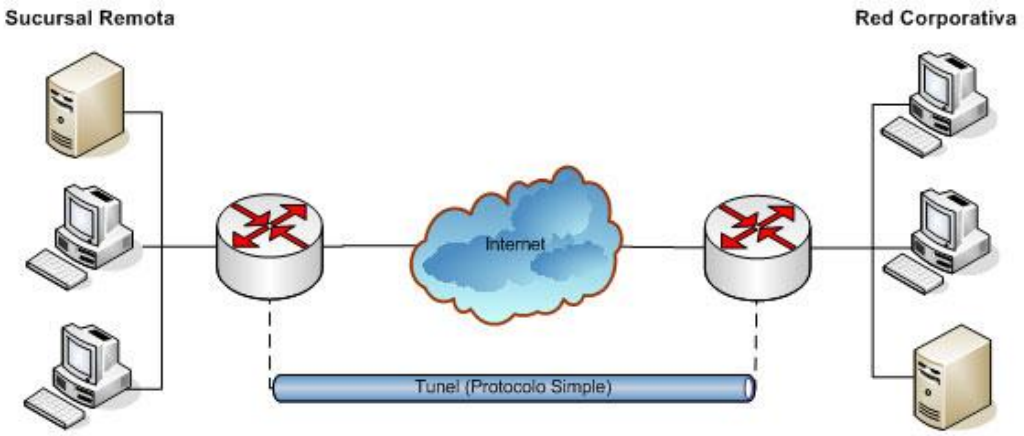


Figura 11.14 VPN-on-demand túnel router a router.

Túneles de multiprotocolo de VPN-ON-DEMAND. Esta implementación es una extensión lógica de VPN-ON-DEMAND porque soporta múltiples protocolos de túnel entre dos sitios a través de Internet. Cuando un cliente no-IP envía una petición para una sesión VPN, un túnel "transparente", el cuál no es específico para cualquier protocolo de túnel, es establecido entre los routers en los dos extremos, los datos IP son entonces enviados a través del túnel de la Internet o cualquier otra red pública hacia el router de destino.

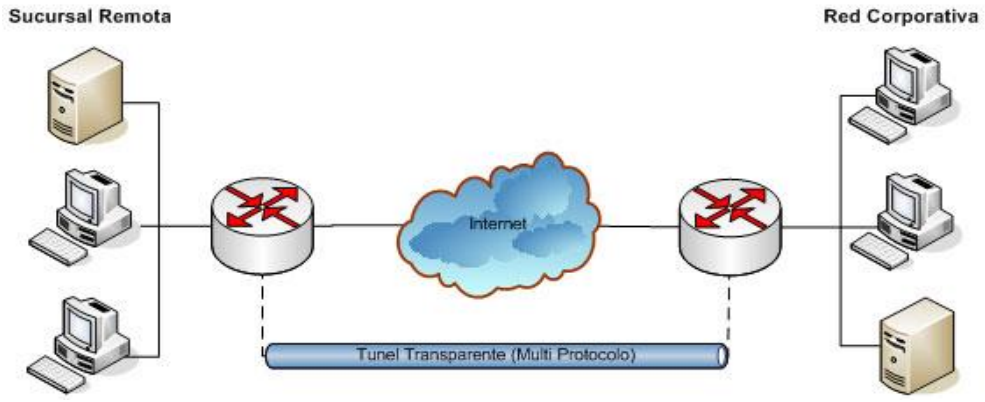


Figura 11.15. Túnel multiprotocolo router a router VPN-on-demand.

Sesiones encriptadas VPN-ON-DEMAND. En esta implementación, un túnel separado para cada petición es establecido en medio de los routers de los extremos a pesar de que las peticiones de conexión múltiples son establecidas para el mismo sitio remoto. Como resultado de múltiples túneles separados que existen simultáneamente entre dos sitios, cada sesión está individualmente encriptada. La desventaja principal de esta arquitectura VPN es que genera gastos generales grandes.

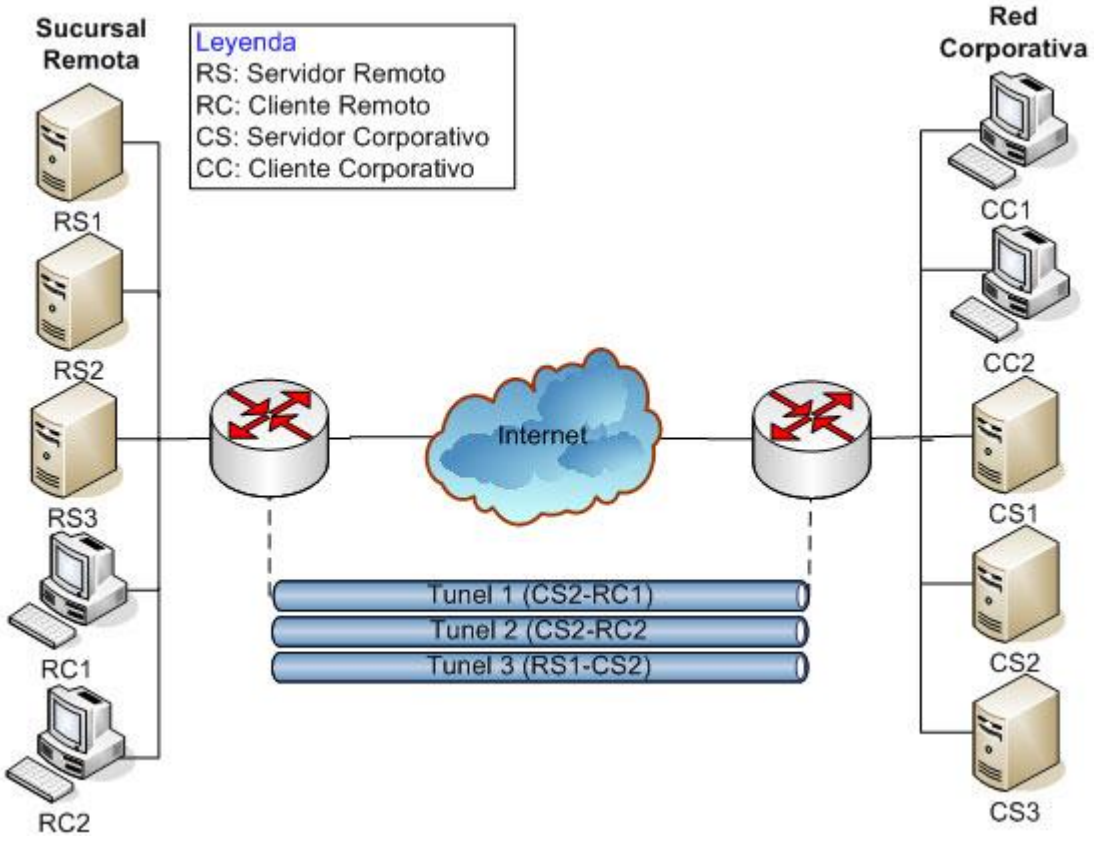


Figura 11.16. Sesiones encriptadas VPN-on-demand router a router.

11.9.2. VPN Firewall a Firewall.

A diferencia de una arquitectura VPN router a router, las VPN firewall a firewall son establecidas entre dos firewalls. Las VPN Firewall a Firewall pueden ser implementadas en las siguientes formas:

a. **Los túneles de VPN-ON-DEMAND.** Esta implementación firewall a firewall es muy parecida a la implementación del túnel de VPN-ON-DEMAND router a router excepto porque firewalls son usados en ambos extremos, provee mas seguridad, además, los administradores de red pueden imponer más restricciones estrictas. Con la ayuda de firewalls, el tráfico también puede ser más estrictamente auditoreado.

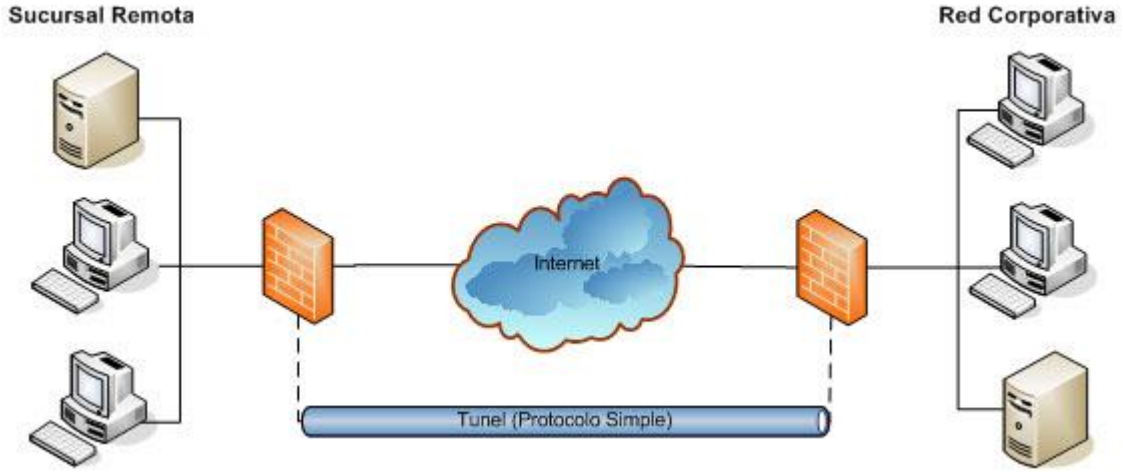


Figura 11.17. Túnel Firewall a Firewall de VPN On Demand

b. **Los túneles multiprotocolo de VPN-ON-DEMAND.** Esta implementación firewall a firewall se ocupa en el problema asociado con la diferencia de firewalls en los dos extremos comunicantes: Los firewalls difererentes no pueden comunicarse exitosamente en un ambiente basado en VPN. Los Firewalls en ambos extremos debe soportar protocolos similares para filtrar tráfico que pertenece a protocolos diferentes. Generalmente, IPSec sirve para este propósito porque soporta túneles multiprotocolo como también firewalls, sin embargo, el requisito en este caso es que el otro extremo debe ser compatible con IPSec.

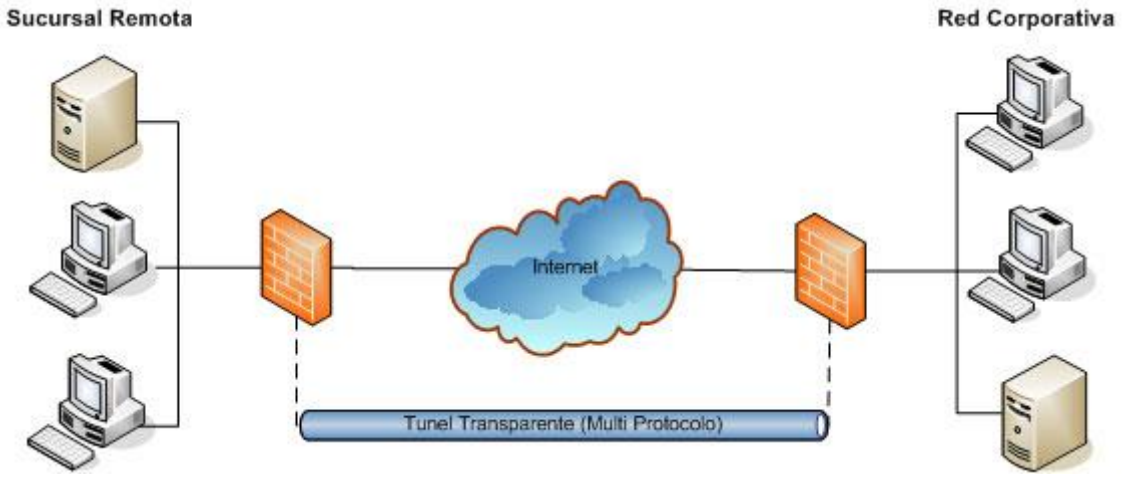


Figura 11.18. Los túneles de firewall a firewall de multiprotocolo de VPN-ON-DEMAND.

11.9.3. Las Client-initiated VPN

En las client-initiated VPN, a diferencia de los dos tipos previos de VPN, el mecanismo de administración de la encriptación y el túnel es instalado en el cliente VPN, como consecuencia, los clientes VPN juegan un papel importante en el establecimiento de los túneles, de ahí el nombre client-initiated VPN. Estas VPN pueden ser clasificadas en las siguientes categorías:

a. **Las VPN cliente a firewall/Router.** En esta implementación, la sesión VPN es negociada entre el cliente y el firewall, el firewall en este caso debe soportar el manejo de peticiones iniciadas por cliente para una sesión VPN, este modelo impone una carga enorme de procesamiento en el cliente por la distribución de llaves, el manejo y el vínculo de seguridad altamente complicado de procesar, además, el cliente debe afrontar la carga adicional de poder comunicarse con una gran variedad de sistemas operativos y plataformas.

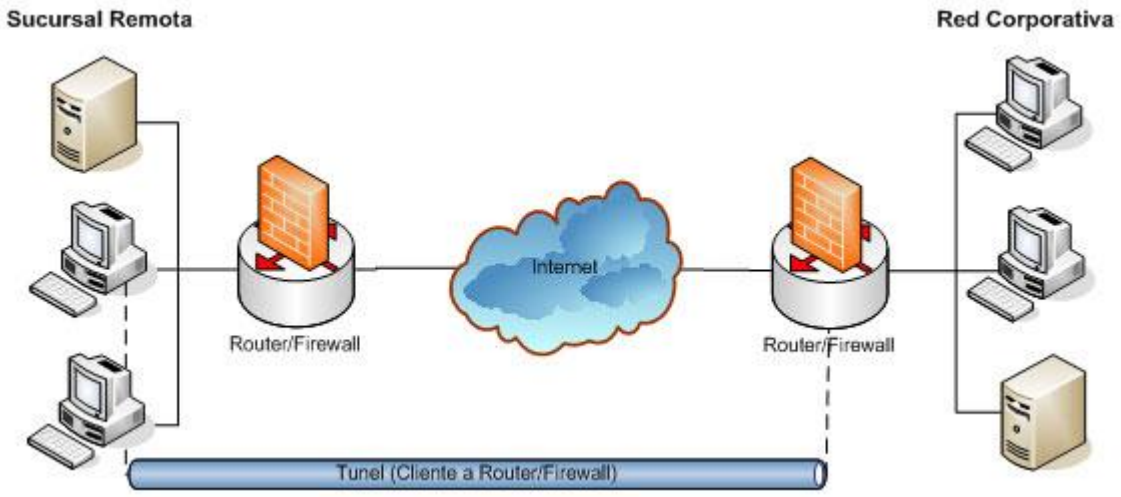


Figura 11.19. La arquitectura VPN cliente a firewall.

b. **Las VPN cliente a servidor.** En esta implementación firewall a firewall una sesión end-to-end VPN es establecida entre el origen de la petición y el procesador de la petición, otra vez, este modelo impone una carga enorme de procesamiento al cliente, sin embargo, es bastante más seguro que una VPN cliente a firewall porque el proveedor intermediario del servicio, cuyos servicios ayuda al cliente a conectarse al servidor remoto, no sabe acerca del túnel, esto reduce las oportunidades de ataques del túnel.

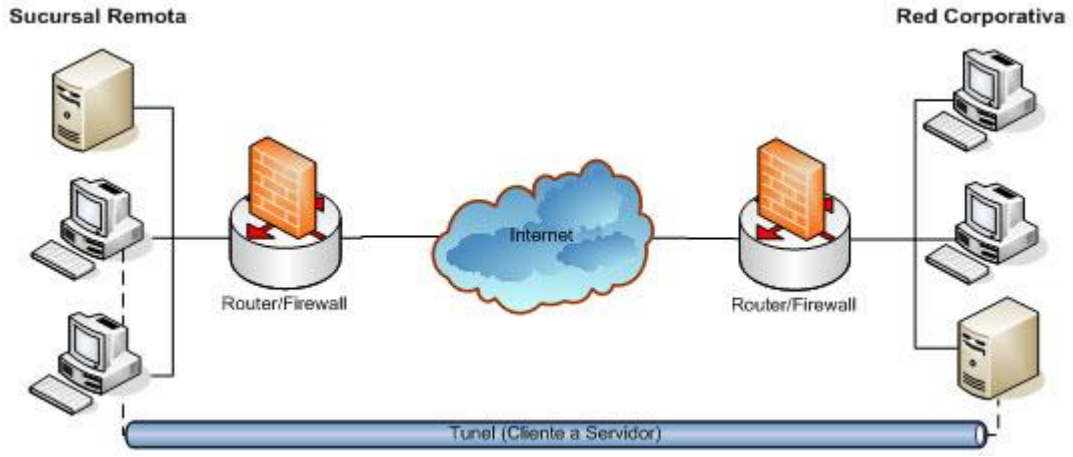


Figura 11.20. La arquitectura VPN cliente a servidor.

11.9.4. Las VPN dirigidas.

A diferencia de todos los demás arquitecturas VPN, las VPN dirigidas no hacen uso de túneles bidireccionales para la comunicación segura, en lugar de eso, un túnel unidireccional es establecido entre los dos extremos que se comunican. Las VPN

dirigidas son diferentes a otras arquitecturas VPN en más de una forma, los datos son encriptados en las VPN dirigidas en la capa cinco del modelo OSI, la capa de sesión. El protocolo más comúnmente destinado para este propósito es SOCKS v5.

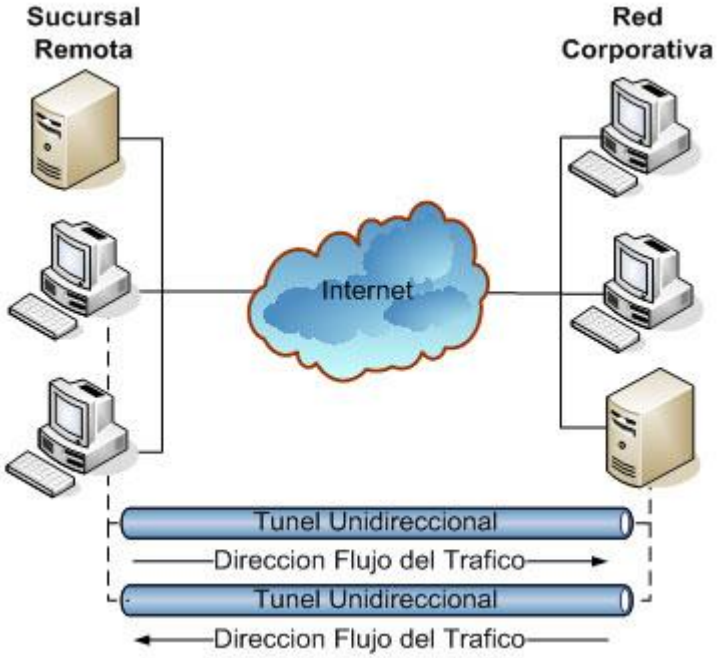


Figura 11.21. La arquitectura VPN dirigida.

Cuando se compara el túnel bidireccional, las VPN dirigidas proveen seguridad mejorada en las siguientes formas:

- En una relación de confianza mutua (doble sentido). cuando un hacker gana acceso a una red, todos los demás redes conectadas pueden ser afectadas, porque el hacker puede ganar acceso a estas redes conectadas con la ayuda del túnel de doble sentido, este no es el caso con las VPN dirigidas, debido al hecho que el flujo del tráfico es unidireccional en las VPN dirigidas, la confianza de doble sentido no es asumida, como consecuencia, aun si un hacker gana acceso a un lado comunicante, la probabilidad de amenaza es disminuida a la mitad por el uso de túneles de una sola vía.
- El control de acceso en un túnel bidireccional que se basa en direcciones fuente y destino, en contraste, al control de acceso en las VPN dirigidas puede basarse no sólo en direcciones de la fuente y del destino, sino que

también con base en otros parámetros, algo semejante como la identificación de usuario, el tiempo, y la aplicación. Las VPN dirigidas también pueden basar el control de acceso en el contenido de los paquetes de datos.

- La autenticación de usuario es más rigurosa en las VPN dirigidas con servidores RADIUS, routers, gateways, y firewalls que autentican a un usuario remoto, el servidor VPN (también así como el cliente) es capaz de autenticar el otro extremo, sin embargo, esto no es el caso con otras arquitecturas VPN. Las peticiones VPN son puestas en el túnel a través de una serie de dispositivos intermedios – NAS, routers, firewalls, etc; que basan su autenticación en direcciones IP origen y destino, esta vía de entrada bidireccional usada en otras arquitecturas le hace fácil al hacker monitorear una dirección IP.
- La encriptación en las VPN dirigidas se basa en la capa de sesión, la cual puede soportar una gran variedad de mecanismos de encriptación, como consecuencia, la encriptación en las VPN dirigidas es bastante más elaborada que en otras arquitecturas VPN.

11.10. ARQUITECTURAS VPN BASADA EN CAPAS.

Dependiendo de la capa del modelo OSI en el cual la solución VPN funciona, las VPN pueden ser clasificadas en las siguientes dos categorías:

- Las VPN de la capa de enlace
- Las VPN de la capa de red

11.10.1. Las VPN de la capa de enlace.

Como el nombre sugiere, las VPN de la capa de enlace usan conectividad de la capa de enlace. Las transacciones de las VPN de la capa de enlace son limitadas a una

red local porque usan direcciones MAC; Por consiguiente, las VPN de capa de enlace son funcionalmente similares a las redes privadas.

Basados en las tecnologías de capa de enlace, las VPN de capa de enlace son de los siguientes cuatro tipos:

- **Conexiones virtuales Frame Relay.** Las conexiones virtuales basadas en Frame Relay usan la infraestructura conmutada de las redes privadas, a las cuales se conectan. La diferencia principal entre conexiones virtuales y conexiones dedicadas es que en conexiones virtuales, los dos extremos usan un registro del tiempo adaptable de datos durante las transmisiones. Como consecuencia, la tasa de transmisión está ajustada según la aplicación y los requisitos de la señal. La ventaja principal de esta tecnología VPN es que es barata y garantiza Committed Information Rate (CIR).
- **Conexiones virtuales ATM.** Las conexiones virtuales basadas en ATM son realmente similares a las conexiones virtuales basadas en Frame Relay, sin embargo, estas conexiones usan la base de la infraestructura en la que se basa ATM de redes privadas. Estas conexiones virtuales también tienen en su haber una falta de sincronización del reloj de datos, las conexiones virtuales ATM son relativamente más rápido y le ofrece mejor desempeño. Por consiguiente, las conexiones virtuales ATM son más caras que las conexiones virtuales Frame Relay.
- **Multiprotocolo sobre ATM (MPOA).** Las conexiones VPN basadas en MPOA se basan puramente en la infraestructura ATM, sin embargo, pueden soportar protocolos múltiples porque están bajo la dependencia de routers localizadas al borde de la red privada para determinar el camino de reenvío dentro de la red ATM, esta metodología no ha ganado mucha popularidad porque la infraestructura base es ATM, lo cual no podría ser aceptable en una red híbrida que usa diversas tecnologías de sistema de redes.
- **Multiprotocol Label Switching (MPLS).** MPLS provee una manera efectiva de destacar las VPNs basados a IP a través de redes WAN basadas en ATM. La VPN MPLS la constituye el router la VPN la tabla especifica de ruteo VPN usando protocolos de VPN que incluyen a BGP, etcétera. Cada ruta está

entonces asignada una etiqueta. Esta etiqueta la información de ruteo que es luego remitido a todas las routers adjuntos. Durante una transmisión, el primer dispositivo MPLS que recibe estos paquetes IP encapsula estos paquetes IP usando las etiquetas MPLS. Subsiguientemente, la etiqueta MPLS, y no el encabezado IP, sirven para encaminar los paquetes a través de la infraestructura basada en ATM. En el borde de la red interna, cuándo el paquete está a punto de acceder a la infraestructura basada en IP (como la Internet), la etiqueta MPLS es removida.

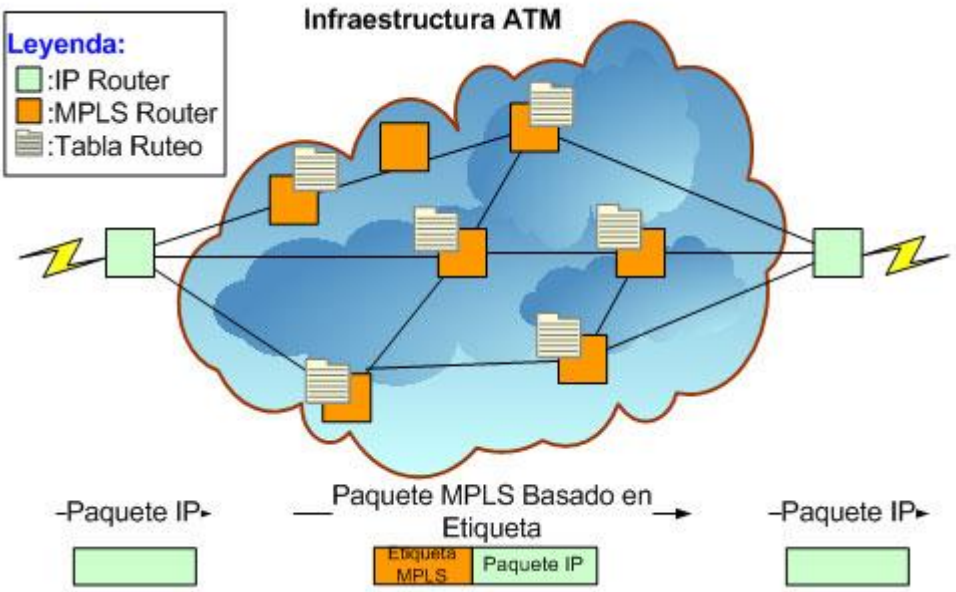


Figura 11.22. VPN MPLS de capa de enlace.

11.10.2. Las VPN de la capa de red.

Las VPN de la capa de red, también conocida como VPN de capa 3, usan la funcionalidad de la capa de red y pueden ser organizados en las siguientes categorías:

- **El modelo Peer-VPN.** En el modelo Peer-VPN, el camino que fomenta la capa de red es calculado en una base de salto a salto, simplemente, el camino es considerado en cada router en el camino hacia la red destino, por consiguiente, todos los routers en el camino de transferencia de datos son considerados como iguales.

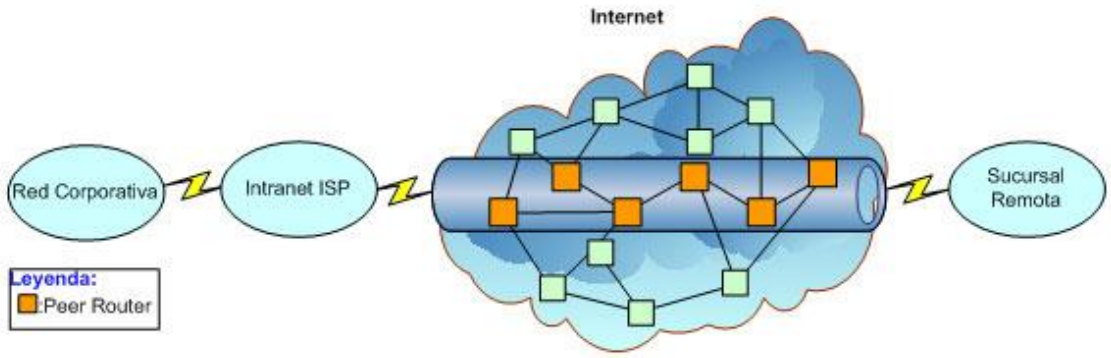


Figura 11.23. La arquitectura de peer-VPN.

- **El modelo Overlay VPN.** A diferencia del modelo de peer-VPN, los modelos Overlay VPN no calculan el camino a la red destino en una base de salto a salto, en lugar de eso, la infraestructura intermedia de la red interna es utilizada como un "atajo" para el siguiente router en el camino de transmisión de datos. Las VPN basados en ATM, Frame Relay VPN y VPN utilizando tecnología de túnel son algunos ejemplos del modelo Overlay VPN.

  Las VPN de capa 3 son también popularmente llamadas *Virtual Private Dial Networks*(VPDN), las VPN de capa 3 comúnmente usan dos tecnologías de capa 2, PPTP y L2TP para crear el túnel. Las VPDN también usan IPSec, lo cual ya ha sido establecido como el estándar VPN de facto porque ofrece capacidades de autenticación y de encriptación.

11.11. ARQUITECTURAS DE VPN BASADA EN CLASES.

Según una clasificación propuesta en un boletín por VPNet Technologies S.A., Las VPN pueden estar divididas en cinco clases, desde la Clase 0 hasta la Clase 4, dependiendo del propósito, el tamaño, el alcance, y la complejidad del esquema VPN.

11.11.1. VPN clase 0.

Las VPN que pertenecen a la Clase 0 son orientadas para organizaciones pequeñas con una red local, limitado para un solo sitio. También, el número de usuarios remotos que acceden a la red de la organización es limitado a 50 o menos. Como consecuencia, las VPN Clase 0 son más fácil de implementar y mas baratas.
Los requisitos mínimos de una VPN Clase 0 incluyen lo siguiente:

- Un servidor VPN con al menos Windows 2000
- Un cliente VPN con al menos Windows 95/98
- Un protocolo de túnel, como PPTP
- Capacidades de filtración de paquetes ofrecida por un router, gateway o firewall.
- Una opción de acceso, como DSL o T1.

La desventaja principal de las VPN que forman parte de esta clase es que son únicamente para túneles locales y no puede soportar conectividad de VPN sitio a sitio, además, las VPN Clase 0 son mas difíciles a la hora de localizar y corregir problemas.

11.11.2. VPN clase 1.

Las VPN clase 1 son más adecuadas para los requisitos de parte de una pequeña a mediana empresa con una red que consiste de dos a 20 redes remotas, además, en promedio al menos 250 usuarios remotos se esperaría a que accedan la red. Estas VPN son bastante más seguras que las de Clase 0 y ofrecen la seguridad IPSec para el túnel de datos así como también un mecanismo de autenticación reforzado del usuario remoto.

Los requisitos mínimos de las VPN Clase 1 incluyen lo siguiente:

Encriptación basado en normas de cifrado de datos.

Manejo de llaves basado en IKE.
Un mecanismo de autenticación de usuario.
Al menos un gateway VPN.
Acceso remoto y software para acceso remoto del cliente.
Una opción acelerada de acceso, como T1 o T3.

Las VPN de esta clase son fáciles de instalar y son eficientes en base a costos. También le ofrecen seguridad mejorada a los datos durante la transmisión, una ventaja añadida de estas es que es posible utilizar las VPN sitio a sitio y las VPN de acceso remoto (a diferencia de la VPN Clase 0), sin embargo, ya que las VPN Clase 1 se basa fuertemente en IPSec, la conectividad podría ser un problema porque las redes externas no podrían soportar IPSec.

11.11.3. VPN Clase 2.

Las VPN clase 2 son más adecuadas para organizaciones de mediana escala con una red que se extiende a través de 10 a 100 sitios remotos. Las VPN que pertenecen a esta clase soportan hasta 500 usuarios remotos, además, esta clase ofrece seguridad mas fuerte que la Clase 1 y todavía se considerada una solución eficiente en base a costos, al igual que las VPN Clase 1, las VPN Clase 2 también soportan conectividad remota sitio a sitio.

Los requisitos principales de una VPN Clase 2 incluyen lo siguiente:

Encriptación basada en IPSec y 3DES.
Manejo de llaves basada en IKE.
Un mecanismo nativo de autenticación de usuario, como Soft Tokens
Al menos dos a cinco gateways de acceso VPN, o un gateway de acceso que pueda soportar 500 sesiones simultáneas.
Mecanismos adicionales de seguridad, como AAA, RADIUS, TACACS, NAT y/o firewalls,
Acceso remoto y software para acceso remoto del cliente.

Opciones de acceso rápido, como T1 o T3.

Aunque esta clase le ofrece más seguridad y conectividad, sus desventajas incluyen una falta de soporte a redes externas, porque se necesita que sean compatibles con IPSec, además, la infraestructura no soporta aplicaciones en tiempo real, como video y audio. El uso de garantía suplementaria, como AAA, RADIUS, y NAT hace la red local más segura; sin embargo, conlleva una carga adicional para el administrador de red.

11.11.4. VPN Clase 3.

Las VPN clase 3 son más adecuadas para organizaciones de medina a gran escala con una red que se extiende a través de varios centenares de sitios remotos, las VPN que forman parte de esta clase pueden soportar a hasta unos mil usuarios remotos. La seguridad ofrecida por esta clase es comparable a la seguridad de Clase 2. Las VPN clase 3 también soportan redes externas además de conectividad remota sitio a sitio. El beneficio más importante ofrecido por esta clase es soporte para el tráfico crítico a retraso y aplicaciones, como videoconferencias. Las VPN que forman parte de esta clase son caras.

Los requisitos mínimos de la VPN Clase 3 incluyen lo siguiente:

La conectividad del ISP con una SLA bien definida.
El servicio centralizado de directorio, como X.500 o LDAP.
Encriptación de datos basado en IPSec y 3DES.
Manejo de llaves basado en IKE.
Un mecanismo nativo de autenticación de usuario, como Soft Tokens y Smart Cards.
Al menos diez a 20 gateways de acceso VPN o un gateway de acceso que pueda soportar hasta 1000 sesiones simultáneas.
Mecanismos adicionales de seguridad, como AAA, RADIUS, TACACS, NAT, y/o firewalls en el sitio principal y todas las grandes sucursales remotas.

Servicios de certificado interno.
Una política de acceso remoto bien definida.
Acceso remoto y software para acceso remoto del cliente.
Opciones de acceso rápido, como RDSI y xDSL junto con T1 o T3.

La desventaja principal de esta clase es que las VPN que forman parte de esta clase son difíciles de manejar, monitorear, configurar e implementar porque los recursos de la organización se esparcen a través del globo, además, es de mucha importancia tener un diseño bien definido y a fondo, sino esta solución cara no podría vivir a la altura de las expectativas.

11.11.5. VPN Clase 4.

Las VPN clase 4 son más adecuadas para organizaciones de gran escala con una red que se extiende a través de miles de sitios remotos. Las VPN que forman parte de esta clase pueden soportar decenas de miles de usuarios remotos. La seguridad ofrecida por esta clase es la máxima, además, esta clase es la más dimensionable y ajustable al crecimiento futuro. Como consecuencia, Las VPN que pertenecen a la Clase 4 son muy caras. Las VPN clase 4 soportan conectividad remota sitio a sitio.
Por las opciones aceleradas de acceso que se usan en las VPNs Clase 4, pueden soportar transacciones de comercio electrónico así como también transacciones en tiempo real, audio y vídeo.

Los requisitos mínimos de las VPN Clase 4 incluyen lo siguiente:

- Conectividad a un ISP con una SLA bien definida.
- Servicio centralizado de directorio, como LDAP.
- Encriptación de datos basado en IPSec y 3DES.
- Manejo de llaves basado en IKE.
- Un mecanismo nativo de autenticación de usuario, como Soft Tokens y Smart Cards.

- Al menos diez a veinte gateway de acceso VPN, o un gateway de acceso que pueden soportar más que 5000 sesiones simultáneas.
- Alta capacidad de redundancia y ancho de banda.
- Una política de acceso remoto bien definida.
- Mecanismos adicionales de seguridad, como AAA, RADIUS, TACACS, NAT, y/o firewalls en el sitio principal y todas las sucursales remotas grandes.
- Servicios de certificado interno.
- Acceso remoto y software para acceso remoto del cliente.
- Opciones de acceso rápido, como RDSI y xDSL junto con T3 y OC3.

La desventaja principal de esta clase es que es sumamente complicada y muy difícil de manejar. Sólo profesionales altamente calificados pueden manejar la tarea de administración.

También, el gran tráfico es otro problema principal asociado con estas VPN, a pesar de las medidas para controlarlo y manejarlo.

11.12. CRITERIOS DE ELECCIÓN DE UN TECNOLOGIA DE VPN.

Cada esquema de VPN se puede implementar en ciertos ambientes y bajo ciertas circunstancias, entonces se hace necesario establecer algunos criterios, en los cuales basarse para asegurar de mejor manera que la opción elegida es la más conveniente y que realmente cubra las necesidades establecidas.

A continuación se exponen algunas opciones y ambientes en las cuales se recomiendan.

11.12.1. VPN MPLS.

- Se necesita capacidad de mantener los servicios existentes y migrar cuando sea necesario y a un ritmo sostenible hacia una red VPN IP flexible que soporte todo tipo de conexiones.
- Cuando un proveedor de servicio necesite integrar servicios a sus redes de datos de forma fácil y a bajos costos.
- Si se necesita eficiencia en los tiempos en el transporte y elección de rutas, además permitir definir prioridades asegurando la calidad en voz, video y datos críticos.
- Cuando se necesite consolidar contratos con un número menor de proveedores de servicios, para reducir costos y simplificar el soporte, el monitoreo y el pago por la administración de redes.
- Si se necesitan las características de la transmisión de datos sin conexión "entre dos puntos cualquiera" y de la transmisión con conexión punto a punto, a la vez que elimina sus inconvenientes.
- Cuando se necesite escalabilidad y flexibilidad, que permita conectarse con quien se desee y con la calidad de servicio necesaria, aprovechando, al mismo tiempo, las economías de escala de la red central IP global.
- Si se necesita contratar un esquema de VPN Sitio a Sitio de un Proveedor de Servicios.
- Cuando el proveedor de servicios necesita ofrecer niveles diferentes de servicio tales como Calidad de Servicio (QoS) y Acuerdos de Nivel de Servicios (SLA).
- Si se encuentra en esquemas frame relay y ATM y se desea migrar a uno basado en IP.

Desventajas.

- Ya que las MPLS se basan en la red privada del ISP, el alcance del servicio esta limitado a las ubicaciones en las cuales el ISP opera.

11.12.2. IPSec.

- Cuando se necesite garantizar seguridad en comunicaciones privadas sobre redes IP.
- Si se necesita confidencialidad, integridad y autenticidad de las comunicaciones de datos a través de las redes publicas.
- Cuando se necesita implementación transparente con respecto a las aplicaciones que se ejecutan.
- Si se necesita una implementación de VPN Sitio a Sitio.
- Puede usar IPSec con el fin de requerir la autenticación mutua para todos los equipos clientes que tengan acceso a un servidor. Además, puede definir restricciones en la forma en que se permite a los equipos conectarse a un servidor.
- Cuando la organización necesita una infraestructura general que soporte una gran variedad de protocolos, no solo web o acceso de correo.
- Si se necesita controles de seguridad sobre el acceso de la computadora del usuario remoto.

Desventajas.

- No se recomienda para VPN de acceso remoto ya que soporta un número limitado de túneles, además agrega un costo adicional para la administración de cada cliente VPN.

11.13. EJEMPLOS VPN.

11.13.1 Check Point Express.

Problema

Se tiene una empresa con 500 usuarios o menos, se necesita una infraestructura de red flexible y segura para conectar todos los centros y todos los usuarios. Internet

ofrece un entorno de red flexible y económica, pero, para que además sea seguro, necesita una solución que:

- Proporcione el máximo nivel de seguridad para toda la red y a la vez sea fácil de aplicar
- Conecte de forma segura y en todo momento todas las comunicaciones y recursos de la empresa
- Racionalice la administración y el mantenimiento sin aumentar los gastos administrativos.

La solución adecuada

Check Point Express™ ofrece una seguridad excelente a las empresas de hasta 500 usuarios. Es la solución más completa del sector, diseñada para proporcionar seguridad “sin preocupaciones” a las empresas con recursos de seguridad limitados. Al incluir los máximos niveles de control de acceso, protección integrada contra ataques, conectividad con VPN y una potente administración centralizada, el cliente obtiene seguridad integral en una única solución. Además, Check Point Express está diseñado para alta disponibilidad, lo cual refuerza las instalaciones globales de seguridad y garantiza la total continuidad del negocio. Puede ampliar Check Point Express para proteger centros y usuarios adicionales, lo que equivale a una solución de seguridad que se adapta a la red mientras proporciona una excelente protección de la inversión.

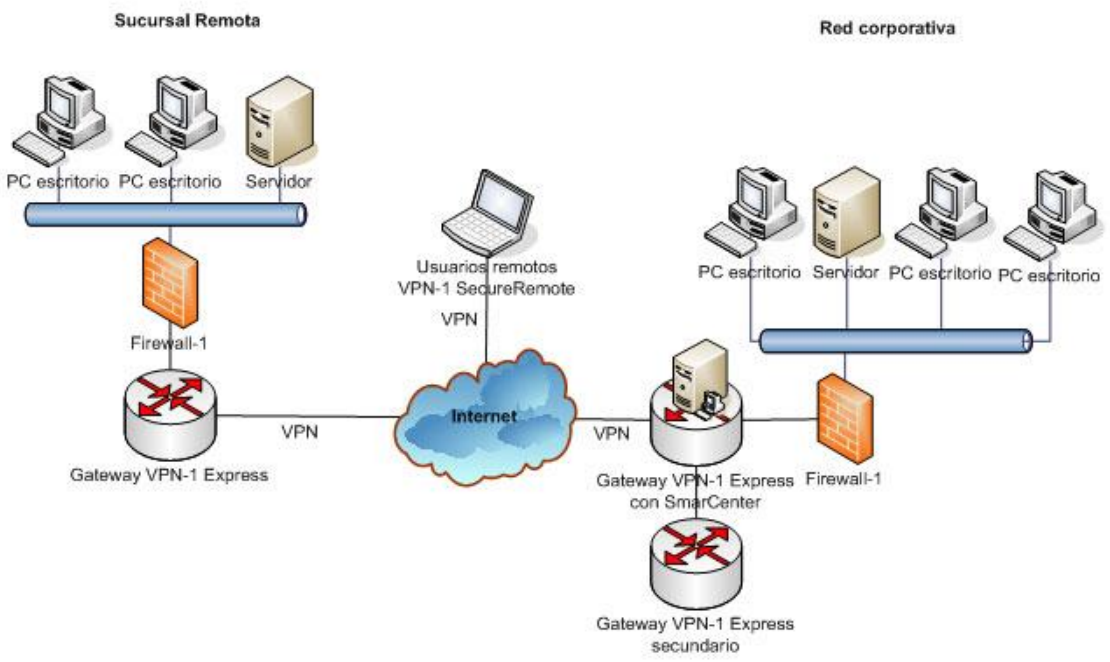


Figura 11.24. Solución Check Point Express.

Check Point Express ofrece seguridad y conectividad totales para las empresas de hasta 500 usuarios y varias sucursales.

CHECK POINT EXPRESS INCLUYE:	
Gateway VPN-1 Express	Protección para las comunicaciones de la empresa por Internet mediante la tecnología de red privada virtual
VPN-1 SecuRemote	Protección para usuarios de red privada virtual con acceso remoto
FireWall-1	Seguridad de categoría empresarial, líder en el mercado
SmartDefense	Protección integrada contra ataques al nivel de redes y aplicaciones
SmartCenter	Administración centralizada de todos los aspectos de la seguridad

Tabla 11.1. Componentes de Check Point Express.

a. Seguridad integrada para máximo nivel, Máximo nivel de control de acceso.

Check Point Express incluye FireWall-1, para proteger todos los servicios habituales de Internet con el producto patentado Stateful Inspection de Check Point. FireWall-1 es compatible, de entrada, con más de 150 aplicaciones, servicios y protocolos predefinidos, incluidas las aplicaciones Web, mensajería instantánea, aplicaciones de

comunicación entre nodos de igual nivel, voz sobre IP, Oracle SQL, RealAudio y servicios multimedia como H.323.

b. Defensa activa integrada contra los ataques.

SmartDefense, como parte de Check Point Express, protege activamente a las organizaciones contra los ataques conocidos y desconocidos a la red y a las aplicaciones. Para ello hace uso de Stateful Inspection y de Application Intelligence. Se integra con la infraestructura de administración y notificación SMART de Check Point para ofrecer una sola consola centralizada que permite la vigilancia de ataques en tiempo real además de la detección, bloqueo, registro, auditoría y aviso de ataques. Las funciones de protección contra ataques, integradas en la solución de seguridad, permiten a la empresa reducir al mínimo las inversiones de capital en productos adicionales de vigilancia del tráfico.

c. Sólida autenticación llave en mano.

Autenticación de alto nivel con disponibilidad inmediata pueden usando certificados One-Click de Check Point. Con una Autoridad de Certificación Interna incluida en Check Point Express, los certificados digitales X.509 se pueden expedir a la gateway VPN-1® Express y a los usuarios de acceso remoto.

Los certificados One-Click ofrecen una autenticación normalizada de doble factor, sin la complejidad y el costo de otras soluciones.

d. Instalación rápida de VPN Fácil creación de VPN

Las organizaciones pueden definir comunidades VPN y establecer los parámetros de seguridad de toda una VPN, incluido el acceso entre centros y acceso remoto. Solamente se definen todos los puntos de conexión de Check Point Express de una comunidad para que se habiliten automáticamente las VPN entre todas las gateways o entre una gateway y un usuario remoto. A medida que se añaden nuevos centros a la comunidad, heredan las propiedades de forma automática y pueden establecer inmediatamente sesiones IPSec seguras con el resto de la comunidad VPN.

e. Niveles de cifrado de máxima complejidad

Además de garantizar la seguridad del acceso a la red, una solución de seguridad debe proteger la confidencialidad de Los datos que se transmiten. Check Point Express, adherido a la norma IPSec, negocia automáticamente el cifrado y algoritmos de autenticación de datos más complejos posibles entre los comunicantes. Esto incluye la norma de cifrado Avanzado (AES) de 128-256 bits y los algoritmos de cifrado de datos Triple DES de 56-168 bits.

f. Compatibilidad con Calidad de Servicio VPN

FloodGate-1 de Check Point, un módulo opcional, configura el tráfico de VPN mediante la asignación de prioridades a las operaciones y usuarios esenciales para el negocio. Optimiza el rendimiento, al permitir a los clientes migrar el tráfico de la empresa desde las costosas líneas dedicadas a las VPN de Internet.

g. Amplia gama de opciones de acceso remoto

Check Point ofrece múltiples soluciones de acceso remoto para permitir a los empleados que trabajan fuera de la central conectarse de forma segura a los recursos de la empresa.

h. Compatibilidad con las tecnologías de acceso remoto sin cliente

Check Point Express es compatible con las VPN sin cliente (SSL) —disponibles con los navegadores Web de uso común, y con los clientes VPN L2TP integrados en los sistemas operativos estándar. Esto elimina la necesidad de invertir en otras soluciones para lograr la compatibilidad con otras tecnologías de acceso remoto.

i. Administración smart sencilla y centralizada.

SmartCenter Express forma parte de la cartera de soluciones SMART (Security Management Architecture) de Check Point y administra las gateways VPN-1 Express. Almacena de manera centralizada la política de seguridad y la distribuye a toda la infraestructura de seguridad. El mantener la política de seguridad en un punto central

elimina la necesidad de mantener cada una de las gateways VPN-1 Express de forma individual, y con ello se reducen la carga administrativa y los errores.

Los administradores usan SmartDashboard, la sencilla interfaz de usuario de SmartCenter Express, para definir y administrar los diversos elementos de una política de seguridad: la seguridad de firewall, las VPN, la conversión de direcciones de red, la calidad del servicio y la seguridad de los clientes VPN.

j. Optimo rendimiento.

Check Point admite toda una serie de opciones de instalación a fin de ofrecer la solución que mejor responda a las necesidades de rendimiento de una red de cualquier tamaño.

Requisitos del sistema.

a. Los gateways VPN-1 Express son compatibles con:

- Windows NT/2000 Server, Sun Solaris, Linux, Check Point SecurePlatform, Nokia IPSO, AIX
- Espacio en disco: 40 MB
- Memoria: 128 MB

b. El servidor de administración SmartCenter Express es compatible con:

- Windows NT/2000 Server/98, Sun Solaris, Linux, Check Point SecurePlatform, Nokia IPSO, AIX
- Espacio en disco: 40 MB
- Memoria: 128 MB

c. SmartDashboard es compatible con:

- Windows NT/Server/XP/ME/98, Sun Solaris
- Espacio en disco: 55 MB
- Memoria: 128 MB
- VPN-1 SecuRemote/Secureclient son compatibles con:

- Windows NT/2000 Server/XP/ME/98/CE, Macintosh, Linux
- Espacio en disco: 20 MB

  Memoria: 64 MB

11.13.2 eTrust VPN

eTrust VPN es una amplia solución de Red Privada Virtual, que ofrece total confidencialidad en las comunicaciones a través de redes públicas y entre servidores situados detrás de un firewall. Permite llevar a cabo de forma fiable las actividades de comercio electrónico (eBusiness) porque garantiza unas comunicaciones seguras con empresas asociadas, oficinas remotas y profesionales que estén de viaje, mientras utiliza Internet para sustituir las costosas líneas telefónicas y enlaces WAN.

a. Seguridad autentificada de punto a punto.

VPN *e*Trust ofrece una solución de seguridad de punto a punto que utiliza una combinación de controles de acceso a la red de cortafuegos, potente cifrado, certificados digitales y autentificación de usuario, para proteger tanto el perímetro como los servidores básicos de la red interna. *e*Trust VPN se instala en servidores de pasarela, así como en servidores de aplicaciones internas y servidores Web. Las políticas de seguridad se definen independientemente de dónde se encuentre el usuario remoto o de cómo acceda el usuario al servidor-mediante el acceso telefónico, a la red local o a Internet.

b. Seguridad potente y transparente

*e*Trust proporciona cifrado de gran intensidad a través de una potente capa de seguridad a nivel de red, sin que sea necesario realizar cambios en las aplicaciones existentes. *e*Trust VPN permite potentes controles de acceso a la red interna para cada uno de sus servidores, que se pueden enlazar entre sí en zonas seguras como "grupos VPN", compartiendo políticas de seguridad comunes. Puesto que las políticas se imponen en cada uno de los servidores como un firewall local, puede impedirse todo acceso no autorizado a la red, cualquier intento por violar la seguridad y generar alertas de seguridad.

*e*Trust VPN también puede funcionar como una solución de seguridad perimétrica, proporcionando un acceso seguro para los usuarios móviles y seguridad de red a red para las redes externas. El trafico asegurado por VPN *e*Trust VPN puede encapsularse en un túnel para lograr su total confidencialidad, o cifrar su carga útil para permitir el funcionamiento de las herramientas de gestión de sistemas y de redes existentes. Se puede proporcionar una solución de confidencialidad total para los protocolos TCP y UDP.

c. Autentificación basada en el usuario

Todos los usuarios deben autentificarse para que se les otorgue acceso a servicios de red restringidos. *e*Trust VPN puede permitir el acceso no autentificado a determinados grupos de la VPN o a toda una red interna. *e*Trust VPN permite el uso de los siguientes métodos de autentificación:

Dominio NT, NDS Novell, SecureID, LDAP 2/3, Windows RADIUS, DCE/Kerberos, certificados digitales X.509v3 PKI y diversos dispositivos biométricos. Puesto que *e*Trust VPN utiliza una arquitectura de conexión abierta, se puede utilizar cualquier dispositivo de autentificación basado en usuario de otros proveedores.

-

d. Fácil administración

Una interfaz intuitiva facilita la configuración y la gestión continua de *e*Trust VPN. La interfaz utiliza asistentes y permite la definición y el mantenimiento detallados de la política de seguridad.

*e*Trust VPN permite la centralización de los controles de acceso a la red, en función de las políticas de seguridad predeterminadas basadas en grupos. Los administradores pueden definir los servicios de red permitidos dentro y fuera de los servidores, seleccionar qué sistemas principales y grupos de trabajo son fiables más allá de esos límites y bloquear el acceso a los no permitidos. *e*Trust VPN incorpora tecnología de cifrado automática que realiza reconocimientos seguros con otros sistemas principales fiables y después cifra automáticamente todo el tráfico en la red.

El cifrado es transparente para los usuarios y lo gestiona centralmente un administrador de VPN.

e. Monitorización en tiempo real y "Audit Trails"

Los monitores de *e*Trust VPN muestran las conexiones de red en tiempo real, confirman el cifrado de datos y muestran registros de auditoria de las conexiones de red. El acceso autentificado se registra centralmente en el Administrador. Una interfaz GUI fácil de usar y amplias posibilidades pueden hacer que cualquier red privada virtual sea fácil de controlar y mantener.

f. Gestión de sistemas y redes

Ofrece potentes posibilidades VPN en toda la empresa. También mejora las posibilidades de seguridad de las herramientas de gestión de sistemas y redes de otros proveedores. Los registros de auditoria de los intentos de acceso, conexiones de red y denegaciones se registran y se transmiten opcionalmente a las aplicaciones de otros proveedores.

g. Entornos soportados

- Microsoft Windows 95, 98
- Microsoft Windows NT 4.0
- Solaris 2.6 +
- AIX 4.3.3 +
- HP-UX 11+

11.13.3. SnapGear SG635.

El SG630/635 es una solución Firewall/VPN de costo muy efectivo empaquetada en una tarjeta PCI. Quitando todos los procesos del Firewall y de la VPN del servidor, el SG630/635 le asegura un alto rendimiento, solución de administración remota y conveniente instalación simplificada. A diferencia de los productos "co-proceso", el SG630/635 es un dispositivo avanzado y que contiene un firewall y VPN multitarea. Incluye un procesador RISC, un acelerador de codificación para el tráfico IPSec de la

VPN y dos interfaces Ethernet para servidor y conexiones LAN. El SG630/635 junta la potencia de una solución SG firewall/VPN mientras que elimina el cableado, elimina los espacios y los requisitos de potencia de un dispositivo firewall externo.

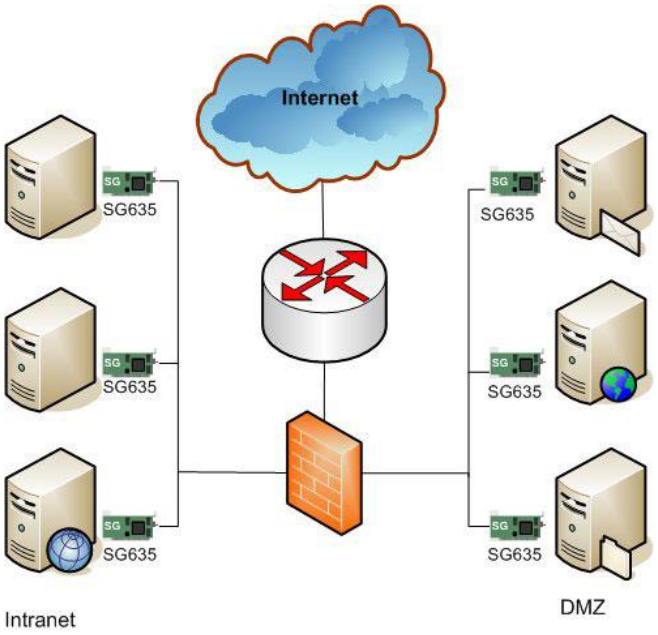


Figura 11.25. Solución SnapGear.

a. Integración IDS Completa.

Todos los dispositivos SG firewall/VPN defienden en contra de ataques DoS y otros ataques comunes, además tiene la capacidad de detectar actividad sospechosa antes que se convierta en una violación de seguridad o acceso indebido a los recursos protegidos.

b. Soporta la estrategia de seguridad Defensa en profundidad.

Los firewall del perímetro son efectivos deteniendo intrusiones de redes externas pero no pueden proteger de ataques que se originan dentro de la red que se protege. El SG635 hace posible esta protección con firewalls incrustados que protegen los host y los servidores críticos.

Múltiples adaptadores SG635 pueden ser desplegados a través de una red para crear un sistema distribuido robusto basado en firewall que continua funcionando aun cuando un host falla. Todos los Firewall SG pueden ser configurados con el Central Managment System (CMS).

Para permitir acceso público transparente, Web, e-mail y servidores FTP, usualmente se ponen en una red frontal o DMZ que impone relativamente pocas restricciones de acceso. El SG635 hace esto posible asegurando cada uno de los servidores mientras conserva el acceso transparente desde el Internet, también puede proteger servidores críticos en la red corporativa o en el ambiente del proveedor de servicios de aplicación.

c. Características

- Firewall de estado de empaquetamiento dinámico en una tarjeta PCI para asegurar sistemas de escritorio y servidores.
- Completamente integrado a VPN basadas en IPSec.
- Cliente y servidor basado en VPN PPTP
- Licencia de usuario ilimitada y sin restricciones.
- Consola Web para la configuración y administración.
- Compatibilidad completa con dispositivos CyberGuard y otros dispositivos de seguridad estándar.
- No se requiere software de terceros.

d. Recomendado para.

- Organizaciones que desean establecer la estrategia de seguridad Defensa en profundidad.
- Ambientes donde la integridad de los host y servidores no pueda ser controlada o confiable.
- Organizaciones con servidores y aplicaciones Web.
- Organizaciones que proveen Web hosting.

- Organizaciones que pretenden demostrar que cumplen con los requerimientos reguladores concernientes a la privacidad y acceso a información personal.

e. Plataformas soportadas:

- Windows 2000 server and client
- Windows 2003 server
- Windows XP
- Linux

11.13.4. NetScreen 500.

a. Vista general del producto

El NetScreen-500 es un sistema de seguridad con finalidad integrada y de alto rendimiento diseñado para proporcionar una solución flexible y de alto rendimiento a los sitios centrales de empresas medianas y grandes y a proveedores de servicios.
El sistema de seguridad NetScreen-500 integra firewall, VPN y funcionalidad de administración de tráfico en un chasis modular de perfil bajo.

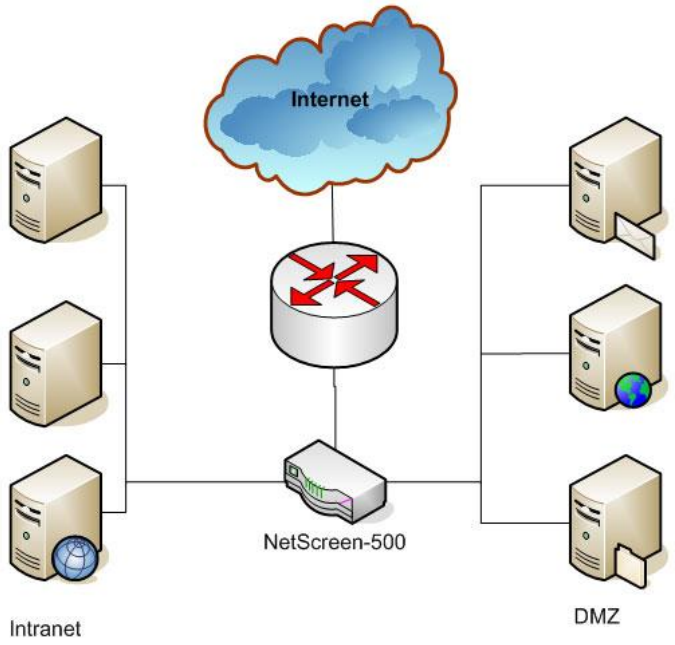


Figura 11.26. Solución NETScreen 500.

b. Firewall

El firewall de NetScreen utiliza tecnología basada en inspección de estado para proporcionar seguridad contra ataques externos e internos. Todas las interfaces, físicas y virtuales, admiten rechazo de servicio (DoS) y funciones de prevención de ataques. Esto brinda una mayor flexibilidad y seguridad a las redes actuales mediante:

- Solución totalmente integrada con hardware, sistema operativo y Firewall de seguridad optimizada, que suministra un mayor nivel de seguridad y rendimiento que las soluciones de software conectadas libremente.
- Amplias capacidades de DoS y prevención de ataques, incluidos ataque SYN, inundación ICMP, análisis de puerto, y otros; combinadas con iniciación acelerada de sesión de hardware, proporcionan protección aun en entornos de red de gran exigencia.
- Traducción de direcciones de red (NAT), de direcciones de puerto (PAT), que protegen direcciones IP internas no enrutables, así como un modo transparente, en el que el dispositivo funciona como un puente de seguridad IP de Capa-2.

c. Red privada virtual (VPN)

Además de un firewall de inspección de estado, el NetScreen-500 es una solución VPN completa. Los túneles VPN se pueden iniciar o terminar en cualquier interfaz, permitiendo la implementación avanzada de VPN, como el aseguramiento de LAN inalámbricas con IPSec para encriptación y autenticación. La naturaleza integrada del ScreenOS permite la inspección total del tráfico de VPN tras las desencriptación y la posterior encriptación, si fuera necesario, para la entrega final. El sistema NetScreen-500 brinda sólidas soluciones VPN, y admite redes VPN con IPSec redundantes y fiables (además de alta disponibilidad entre dos dispositivos), incluidos:

- Puertas de enlace VPN redundantes, que permiten al administrador configurar múltiples definiciones de puerta de enlace para un túnel VPN determinado con detección y reemplazo de componentes con fallas de sistema de puertas de enlace cuando una de ellas no está disponible.
- Interfaces de túnel VPN que permiten el enrutamiento dinámico para elegir el túnel apropiado en función de las decisiones de enrutamiento.
- Compatibilidad absoluta con VPN de acceso remoto, incluida la compatibilidad con XAUTH para autenticación de usuarios de acceso telefónico.

d. Administración de tráfico.

El NetScreen-500 permite a un administrador de red supervisar, analizar y asignar el ancho de banda utilizado por varios tipos de tráfico de red en tiempo real, ayudando a asegurar que el tráfico esencial del negocio no se vea afectado por la navegación Web u otras aplicaciones de menor importancia. En entornos de proveedores de servicios, esto también permite a un administrador proporcionar servicios diferenciados cuando existe una conexión compartida. La administración de tráfico se puede configurar sobre la base de cada directiva, en función de la dirección IP, el usuario, la aplicación, o la hora del día. Para cada directiva se puede definir ancho de

banda garantizado, ancho de banda máximo, y niveles de prioridad. Además, permite a NetScreen-500 señalizar la calidad del servicio (QoS) a una red MPLS.

e. Virtualización (sistemas virtuales, VLAN y zonas de seguridad)

Los sistemas de seguridad de NetScreen proporcionan varias funciones de virtualización que permiten la partición lógica del sistema en dominios de seguridad independiente para la separación de tráfico, directivas y administración. La segmentación del tráfico tiene lugar a nivel de la interfaz, mediante VLAN 802.1Q, o con subredes de dirección IP y sistemas virtuales. Las zonas de seguridad agrupan interfaces, tanto virtuales como físicas, en una red lógica interna.

f. Alta disponibilidad

El sistema NetScreen-500 proporciona la solución integrada más completa de alta disponibilidad en materia de seguridad. Con el protocolo de redundancia de NetScreen (NSRPv2), el sistema NetScreen-500 se puede implementar en entornos de red en malla completa, así como en grupos de redundancia activo/activo (reparto de carga) con firewall de estado y conmutación por error VPN. Los beneficios incluyen:

- Conmutación por error subseguido entre interfaces o dispositivos
- El reparto de carga activo/activo ofrece una mayor capacidad de ráfagas que el activo/pasivo y asegura que ambos dispositivos trabajen correctamente y permitan que pase el tráfico.
- Las configuraciones en malla completa permiten las rutas de acceso físicas redundantes en la red
- Proporciona clústeres sin liderazgo para evitar un único punto de error.

g. Características principales

- **Sistema de seguridad multifunción.**

  Solución integrada de seguridad de red con pared de fuego de inspección de estado, sólidas protecciones DoS, VPN con IPSec de alto rendimiento, y capacidades de administración de tráfico.

- **Sistema modular flexible.**

  Sistema de seguridad de alto rendimiento con finalidad integrada que ofrece soluciones flexibles y ampliables para empresas medianas a grandes y portadoras.

- **Rendimiento fiable**

  El rendimiento de la pared de fuego se puede ampliar a 700 Mbps y el rendimiento de la VPN 3DES, a 250 Mbps, aún con tráfico pesado, grandes sesiones simultáneas, o una gran cantidad de túneles VPN.

- **Sistemas virtuales**

  La partición lógica del sistema en dominios de paredes de fuego individuales o de VPN para segmentación de tráfico, directivas y administración permite el control de la seguridad en departamentos o clientes múltiples desde un único sistema.

11.13.5. Nokia Firewall/VPN

Protege y extiende el perímetro de la red de forma segura, solución confiable que es fácil de instalar y administrar.

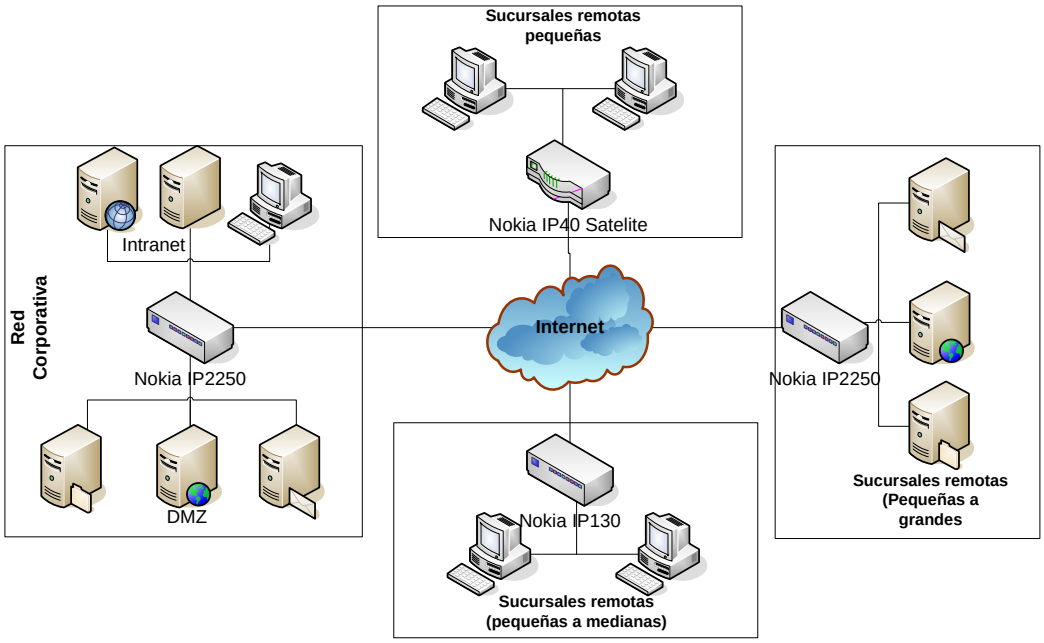


Figura 11.27. Solución Nokia.

a. Solución de seguridad integrada.

Nokia entrega una combinación de aplicaciones de firewall y VPN líder en el mercado, con un SO propietario y endurecido con plataformas de alto desempeño. Incluye una ingeniería de inspección de estado que puede inspeccionar el tráfico de la capa de aplicación, además, con la capacidad de inspección de paquetes a profundidad puede detectar y prevenir ataques a nivel de aplicación proporcionando un ambiente seguro a todos los niveles.

b. Nokia y Check Point

Nokia y check point comparten una relación estrecha que combina técnicas sin precedentes para entregar las mejores prácticas de seguridad.

c. Soluciones de seguridad Nokia IP.

Las plataformas de seguridad de Nokia combinan la seguridad líder del mercado en software y ruteo IP proporcionando soluciones de seguridad de alto desempeño.

d. Características Nokia IP2250.

Rendimiento

- Redirección Firewall (7.5 Gbps)
- Redirección VPN (1.8 Gbps)
- Redirección de conexiones por segundo (47k CPS)

Seguridad

- Acceso administrativo seguro
- Modos de acceso lectura/escritura y solo lectura.
- SSH (seguridad Telnet y FTP)
- SSL/TLS (Seguridad http) RFC 2246
- S/Key (clave de un tiempo) RFC 1760
- Listas de control de acceso
- Administración de trafico
- Ruteo MD5
- Autentificación (RIPv2) RFC 1723
- Autentificación centralizada
- IPSec nativo (para aplicaciones no-firewall)
- Cliente DNS, cliente y servidor NTP
- Cliente RADIUS, cliente TACACS+

Estándares soportados

- IPSec (RFCs 2401-2411, 2451)
- GRE (RFCs 1701 & 1702) Generic Routing Encapsulation
- Diseñado para soportar NEBS III, and FIPS 140-2

Formas de administración

- SNMP RFC 1157, SNMPv2c, SNMPv3
- Telnet RFC 854
- FTP RFC 959
- SSHv2 (secure Telnet & FTP)
- Servidor HTTP RFC 2068
- SSL/TLS RFC 2246

- Utilidades de línea de comando
- Soportado por el administrador Nokia Horizon.

11.13.6. VPN F-Secure

F-Secure VPN es una solución flexible y de coste aprovechable para obtener los beneficios de Internet comprometiéndose a mantener la seguridad en la misma. Dota a la gestión de la red de túneles entre los puntos de empresa manteniendo el acceso a puntos externos si se quiere. Es mejor usar este paquete junto con un firewall para conseguir un control total sobre el tráfico de datos de toda la organización.

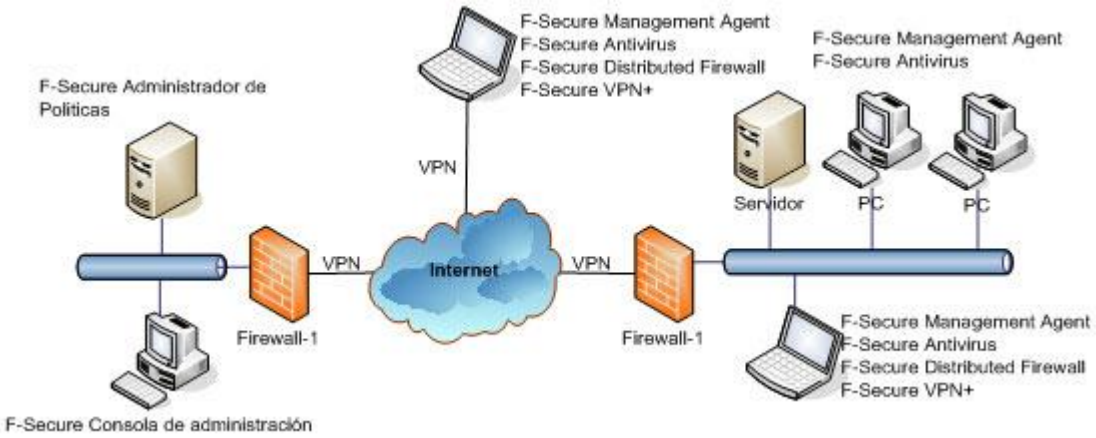


Figura 11.28. Solución F-Secure

a. Características de F-Secure.

Las características principales son las siguientes:

- Fácil de instalar: Requiere muy pocos parámetros de instalación para el Administrador.
- Fácil de configurar: Posee un editor de red gráfico que permite configurar la totalidad de la red VPN desde una simple estación de trabajo.
- Seguro: Usa una extensa variedad de algoritmos de encriptación, tales como DES, Blowfish, RSA, etc.
- Disponible a nivel global, con una fuerte encriptación: Se puede enviar el software encriptado a todo el mundo, sin ningún compromiso.

b. Beneficios de F-Secure

Los beneficios de F-Secure son los siguientes:

- Cualquier PC con ciertos requerimientos mínimos puede utilizar el software de F-Secure VPN.
- La red VPN es dinámicamente ampliable de modo que nuevas LAN se pueden añadir sin demasiada configuración.
- Se pueden usar conexiones a Internet de bajo coste para formar la VPN. Tradicionalmente, las redes privadas virtuales seguras han estado construyéndose usando líneas alquiladas muy caras.
- Automáticamente se encriptan y protegen contra alteraciones, todas las conexiones F-Secure VPN.
- F-Secure VPN se integra con cualquiera de las firewalls existentes.
- F-Secure VPN soporta conexiones Extranet seguras.

11.13.7. Firebox V100: VPN y Gigabit Firewall

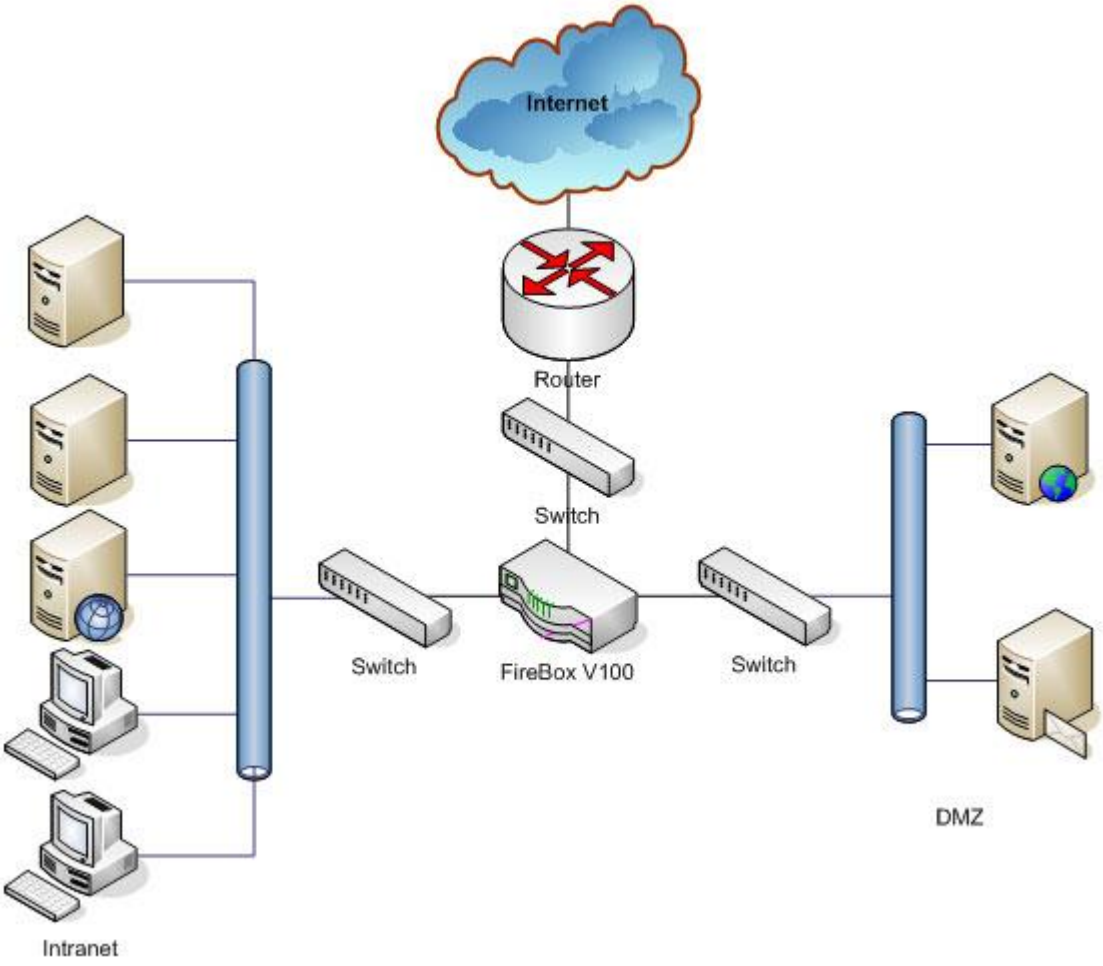


Figura 11.29. Solución FireBox V100

a. Firebox V100 se recomienda para:

- Centros de datos, proveedores de servicios y organizaciones de tamaño mediano que requieren una firewall Gigabit con hasta 20,000 túneles VPN.
- Organizaciones de tamaño mediano que requieren la integración de firewall, VPN, IPS y características de red avanzadas como soporte de VLAN y ruteo estático y dinámico.
- Negocios que necesitan calidad de servicio (QoS), configuración de puertos y configuración de tráfico.
- Redes de misión critica que necesitan soporte de alta disponibilidad y equilibrio de carga.

- Organizaciones de tamaño mediano con múltiples conexiones T3 u OC -3.

b. Características de seguridad.

- Detección de spoof
- IPSec NAT Transversal (NAT-T)
- VPN
- Usuarios móviles usando IPSec o L2TP
- Autenticación de usuarios
- Protección de SYNflood
- Soporte PKI
- Control y definición de alarmas
- Autentificación de acceso remoto
- Servicios de firewall predefinidos
- NAT Estático (SNAT), NAT Dinámico (DNAT), Virtual IP (VIP) y redireccionamiento de puertos.

c. Características de Red.

- Calidad de servicio (QoS).
- Balance de la carga del servidor.
- Soporte VLAN.
- Regulador DHCP.
- VPN de túnel conmutado.
- Ruteo dinámico
- Soporte PPPoE y DHCP

d. Características de administración.

- GUI basada en JAVA.
- Asistente de instalación.

- Interfase de línea de comandos
- Herramientas de diagnostico de red.
- Monitoreo de tráfico en tiempo real.
- Shell Seguro (SSH).
- Rendimiento.
- Rendimiento de Firewall 600 Mbps
- Rendimiento de VPN 300 Mbps
- VPN de Oficina regional 20,000
- VPN de usuarios móviles 20,000

CAPITULO 12 SERVICIO DE SEGURIDAD AAA

En este capitulo se describe brevemente el concepto de AAA y cada uno de los protocolos que podría utilizar para la comunicación, además se proporciona información acerca de las ventajas y desventajas de cada protocolo.

Puntos claves:

- Concepto del AAA y sus características.
- Protocolo TACACS+
- Protocolo RADIUS
- Ventajas y desventajas de los protocolos.

12.1. UN VISTAZO AL AAA.

Colectivamente, autenticación, autorización y contabilidad están referidos como AAA manteniendo funciones importantes pero separadas a la vez.

a. Autenticación determina quien es el usuario, además verifica si el usuario tiene acceso a la red. El propósito primario es prevenir que los intrusos entren a la red corporativa. Esté usa una base de datos de usuarios y passwords.

b. Autorización determina que tiene permitido el usuario hacer mientras se encuentra en la red. La autorización le proporciona al administrador de red la habilidad para limitar los servicios de red hacia diferentes usuarios.

c. Contabilidad rastrea lo que el usuario hizo y cuado lo hizo. La contabilidad puede ser usada para auditar, el cobro por tiempo de conexión o recursos usados.

La información que es administrada por la central AAA se encuentra en una base de datos centralizada y segura la cual es mucho más fácil para manipular la información que esta distribuida a través de muchos dispositivos. Tanto los protocolos RADIUS como TACACS+ son sistemas clientes servidor lo cual permite la comunicación efectiva de la información AAA.

AAA puede ser usado con IPSec para proveer llaves pre-compartidas durante el proceso del protocolo ISAKMP o proveer autenticación por usuario conocida como XAUTH durante el proceso ISAKMP

12.1.1. Filosofía AAA.

AAA esta diseñado para permitir la configuración dinámica del tipo de autenticación y autorización que se desea por usuario o por servicio, se define el tipo de autenticación y autorización mediante la creación de listas de métodos, posteriormente se aplican estas listas de métodos hacia los servicios o interfaces especificas.

Una lista de método es una línea secuencial que define los métodos de autenticación usados para autenticar un usuario. La lista de métodos permite designar uno o más protocolos de seguridad que pueden ser usados para autenticación, además aseguran un sistema de respaldo para autenticación en caso de que el método inicial falle.

El software IOS de cisco usa el primer método listado para autenticar usuarios, si ese método no responde, el software IOS selecciona el siguiente método de autenticación en la lista. Este proceso continua hasta que existe una comunicación satisfactoria con un método de autenticación listado o la lista de métodos de autenticación es agotada, en este caso la autenticación ha fallado.

12.1.2. Acerca de los servicios de seguridad AAA.

AAA es una estructura para un conjunto de configuraciones de tres funciones de seguridad independientes de una manera consistente. AAA provee una manera modular para el desarrollo de los siguientes servicios:

Autenticación: provee un método de identificación de usuarios, incluyendo diálogos para el login y password, desafíos y preguntas, y por ultimo soporte de mensajes.

Autenticación es la manera en que un usuario puede ser identificado con el objeto de verificar si dicho usuario esta permitido para acceder a la red y a los servicios de red corporativa. Se debe configurar la autenticación AAA mediante la definición de una lista nombrada de métodos de autenticación para aplicar posteriormente esta lista a las diferentes interfaces, las listas de métodos define que tipo de autenticación debe ser realizada y la secuencia en que esta debe ser ejecutada.

Todos los métodos de autenticación excepto por el usuario local, línea de password y habilitación de autenticación deben ser definida por el AAA

Autorización: provee el método para el control de acceso remoto incluyendo autorización de un solo tiempo, o autorización por cada servicio, por perfil y listas de cuenta por usuario, grupo de soporte o soporte para IP, IPX, ARA y TELNET.

La autorización trabaja mediante la unión de un conjunto de atributos que describen que es lo que puede realizar el usuario dentro de la red corporativa. Estos atributos son comparados con la información contenida en una base de datos por un usuario dado y el resultado es enviado al servidor AAA para determinar las capacidades y restricciones del usuario actual. La base de datos puede ser localizada en el servidor de acceso, en el router o puede ser accesada remotamente desde un servidor de seguridad RADIUS o TACACS+. Los servidores de seguridad remotos, como los son: RADIUS y TACACS+, solamente los usuarios autorizados con derechos específicos pueden usar pares de asociaciones de valor - atributo (AV) los cuales define que derecho tienen un usuario determinado. Todos los métodos de autorización deben ser definidos a través del AAA.

Al igual que con la autenticación, se debe configurar la autorización AAA mediante la definición de una lista nombrada de métodos de autorización y luego aplicar esta lista hacia las diferentes interfaces.

Contabilidad: provee el método para la recolección y envió de información del servidor de seguridad con el objetivo de facturar, auditar o reportar como por ejemplo: las identidades de los usuarios, comienzos y finalización de tiempo, comandos ejecutados, número de paquetes y número de bytes.

La contabilidad permite rastrear los servicios que los usuarios están accediendo así como la cantidad de recursos que estos están consumiendo. Cuando la contabilidad AAA esta activada el servidor de acceso de red reporta la actividad del usuario hacia el servidor de seguridad RADIUS o TACACS+ (dependiendo de que método de seguridad se haya implementado) en la forma del registro de contabilidad. Cada registro de contabilidad esta comprometido con la contabilidad de pares AV y almacenado en el servidor de control de acceso.

Estos datos pueden ser analizados solamente por el administrador la red corporativa para la facturación de clientes y/o auditoria. Todos los métodos de contabilidad AAA deben ser definidos a través de AAA. Al igual que con autenticación y autorización se debe configurar mediante la definición de una lista de métodos de contabilidad y luego aplicar esta lista a las diferentes interfaces.

AAA actualmente soporta seis tipos de contabilidad las cuales son las siguientes:

- Contabilidad de red.
- Contabilidad de conexión
- Contabilidad de sesiones de terminales ejecutables
- Contabilidad del sistema
- Contabilidad de los comandos ejecutados
- contabilidad de recursos

En muchas circunstancias AAA usa protocolos como lo son RADIUS o TACACS+ para administrar sus funciones de seguridad. Si el router o el servidor de acceso están actuando como un servidor de acceso de red AAA es el medio por el cual se puede establecer comunicaciones entre el servidor de acceso de red y el servidor de seguridad TACACS+ o RADIUS.

Auque AAA es el método primario para el control de acceso (él mas recomendado) el software IOS de cisco provee funciones adicionales para el control de acceso simple que están fuera del ámbito AAA como por ejemplo: autenticación del nombre del usuario local, autenticación de la línea de password y la habilitación del password de autenticación. Sin embargo estas funciones no proveen el mismo grado de control de acceso que es posible alcanzar mediante el uso de AAA.

12.1.3. Beneficios del AAA.

- Flexibilidad incrementada y configuración de control de acceso
- Escalabilidad
- Métodos de autenticación de estandarizados como lo son: RADIUS, TACACS+ y kerberos
- Múltiples sistemas de respaldos

Para mayor información visitar el siguiente sitio:

http://www.cisco.com/en/US/products/hw/optical/ps2011/products_white_paper0900aecd802859a5.shtml

12.2. UN VISTAZO A TACACS+

TACACS+ es un protocolo reciente que provee información y flexibilidad administrativa para controlar la autenticación y autorización de procesos. Tacacs+ es el resultado de la evolución de TACACS y TACACS Extendido (XTACACS).

TACACS+ es facilitado a través de AAA y puede ser habilitado solo a través de comandos AAA.

12.2.1. Funciones claves de TACACS+:

- TACACS+ separa AAA en tres funciones distintas (Autenticación, Autorización y Contabilidad)
- TACACS+ soporta integración de autorización por comando de router con mecanismos de autenticación avanzados, como lo son DES (Data Encryption Standard) y llave de password de una sola vez (OTP- One Time Password)
- TACACS+ soporta 16 tipos de privilegios diferentes (0-15)
- TACACS+ permite el control de servicios, como PPP (Point-to-Point Protocol), interprete de comandos, entrada de usuarios estándar, habilitación, Protocolo ARA (AppleTalk Remote Access), NASI (Novell Asynchronous Services Interface), comandos remotos (RCMD – Remote Command) y un proxy firewall.
- TACACS+ permite el bloqueo de servicios para un puerto especifico, entre los cuales se tienen las siguientes interfaces en un router: TTY o VTY.

Los servicios más comunes soportados por TACACS+ son PPP para IP y él interprete de comandos ejecutables del router usando la consola o puertos VTY. El intérprete de comandos permite a los usuarios conectarse al intérprete de comandos del router y seleccionar servicios como lo son PPP, Telnet, TN3270 o manejo del router mismo.

Muchos servidores TACACS+ están disponibles en el mercado hoy en día, sin embargo, el servidor AAA esta designado específicamente para ser escalable y compatible con los routers de la marca Cisco, servidores de acceso y switches. Por lo tanto, en este caso se utilizan el servidor AAA de Cisco como el servidor de elección de TACACS+.

Cuando esta configurado correctamente, el servidor AAA valida AAA y responde a las peticiones del router y el servidor de acceso con una señal de *pass* o *fail*. El servidor AAA contiene una base de datos interna con la capacidad para soportar hasta 5000 usuarios.

El servidor AAA actúa como un servidor proxy al usar TACACS+ para autenticar, autorizar y contabilizar el acceso a los routers Cisco y los servidores de acceso a la red.

TACACS+ es una aplicación de seguridad que provee validación centralizada de usuarios que intentan ganar acceso a un router o servidor de acceso de red. Los servicios de TACACS+ son mantenidos en una base de datos, los cuales corren en un programa TACACS+ utilizando una estación de trabajo bajo Linux o servidores Windows.

El objetivo de TACACS+ es proveer una metodología para manejar múltiples puntos de acceso a la red desde un solo servicio de administración. La familia de servidores de acceso y routers, (tanto en los routers como en los servidores de acceso) pueden ser servidores de acceso a la red.

Los puntos de acceso a la red habilitan tradicionalmente terminales “tontas”, emuladores de terminales, estaciones de trabajo, computadoras personales y routers en conjunto con otros adaptadores (por ejemplo MODEMS o otros adaptadores ISDN) para comunicarse usando protocolos como PPP, SLIP, CSLIP y ARA. En otras palabras, un servidor de acceso a la red proporciona conexiones a un solo usuario, a una red o subred y a redes interconectadas. Las entidades conectadas a través del servidor de acceso a la red son llamadas clientes de acceso a la red.

El protocolo TACACS+ suministra autenticación entre el servidor de acceso a la red y el servicio de TACACS+ y asegura la confiabilidad porque todos los intercambios del protocolo entre le servidor de acceso a la red y el servicio TACACS+ están encriptados.

Para mayor información acerca del protocolo TACACS+ visitar:

http://www.cisco.com/warp/public/459/tac-rfc.1.76.txt

12.3. UN VISTAZO A RADIUS

El protocolo RADIUS fue desarrollado por Livingston Enterprises, Inc. Como un protocolo de autenticación y contabilidad para un servidor de acceso. La especificación RFC 2138 de RADIUS es un protocolo estándar propuesto y el estándar de contabilidad RADIUS RFC 2139 es informal.

Aunque TACACS+ es considerado ser más versátil, RADIUS es el protocolo AAA por excelencia para las empresas ISP porque este utiliza menos ciclos del CPU y menos intensidad de memoria.

La comunicación entre un servidor de acceso a la red (NAS) y un servidor RADIUS esta basada en el protocolo UDP (User Datagram Protocol). Generalmente, el protocolo RADIUS es considerado un servicio sin conexión. Problemas relacionados a la disponibilidad del servidor, retransmisión y tiempos agotados son manejados por los dispositivos habilitados por RADIUS en ves del protocolo de transmisión.

RADIUS es un protocolo cliente/servidor. El cliente RADIUS es típicamente un servidor de acceso remoto (NAS) y el servidor RADIUS es usualmente un programa en proceso corriendo en una computadora utilizando LINUX o Windows. El cliente pasa la información del usuario hacia el servidor RADIUS designado y actúa en base a la respuesta obtenida. El servidor RADIUS recibe las peticiones de conexión del usuario, autentica al usuario y la información de configuración necesaria hacia el cliente para permitir el acceso del usuario hacia los servicios de la red.

Un servidor RADIUS puede actuar como un cliente proxy hacia otros servidores RADIUS o hacia otra clase de servidores de autenticación.

Para mayor información acerca de RADIUS visitar:

http://www.ietf.org/rfc/rfc2138.txt

12.4. COMPARACIÓN DE TACACS+ Y RADIUS

A continuación en la tabla 12.1 se describen comparaciones entre TACACS+ y RADIUS.

RADIUS	TACACS+
RADIUS utiliza UDP	TACACS+ utiliza TCP
RADIUS encripta solamente el password en el paquete de petición de acceso, es menos seguro.	TACACS+ encripta el cuerpo entero del paquete, es mas seguro.
RADIUS combina autenticación y autorización	TACACS+ utiliza la arquitectura AAA, el cual separa la autenticación, autorización y contabilidad.
Estándar de la industria (creado por Livington)	Propiedad de Cisco
RADIUS no soporta acceso ARA, Protocolo de control protocolo de cuadro Net BIOS, NASI y conexiones PAD X.25	TACACS+ ofrece soporte multiprotocolo
RADIUS no permite a los usuarios controlar que comandos pueden ser ejecutados en el router.	TACACS+ provee dos caminos para controlar la autorización de los comandos del router: uno por usuario o uno por grupo

Tabla 12.1 comparaciones entre TACACS+ y RADIUS

a. UDP y TCP

El protocolo RADIUS utiliza UDP mientras que el protocolo TACACS+ utiliza TCP. TCP ofrece muchas ventajas sobre UDP. TCP ofrece un transporte orientado a conexión, mientras que UDP ofrece una entrega haciendo el mejor esfuerzo. RADIUS requiere variables programables adicionales, como lo son: los intentos de retransmisión y los tiempos agotados para compensar el transporte con el mejor esfuerzo.

- El uso de TCP provee un reconocimiento separado de que una petición ha sido recibida.
- TCP provee indicación inmediata de un servidor caído (o no corriendo) usando paquetes RST. Se puede determinar cuando un servidor se ha caído y se ha vuelto a levantar el servicio si se usan conexiones TCP de larga vida. UDP no puede decir la diferencia entre un servidor que esta fuera de servicio, lento o no existente.
- TCP es más escalable que UDP.

b. Encriptación de paquetes

RADIUS encripta solamente el password en el paquete de petición de acceso desde el cliente hacia el servidor. El resto del paquete esta en texto normal. Otra información como lo es nombre del usuario, servicios autorizados y contabilidad pueden ser capturados por una tercera persona.

TACACS+ encripta el cuerpo entero del paquete pero deja una cabecera TACACS+ estándar. Dentro de esta cabecera hay un campo que indica cuando el cuerpo esta encriptado o no. Para propósitos de depuración, es muy útil tener un cuerpo del paquete en texto normal. Sin embargo, la operación normal encripta completamente el cuerpo del paquete para comunicaciones más seguras.

c. Autenticación y autorización

RADIUS combina autenticación y autorización. Los paquetes de aceptación de acceso enviados por el servidor RADIUS hacia el cliente contienen información de autorización, haciendo más difícil separar la autenticación y la autorización.

TACACS+ usa la arquitectura AAA, el cual separa la autenticación, autorización y contabilidad. Esta arquitectura permite separar las soluciones para autenticación que TACACS+ puede usar aun para autorización y contabilidad.

d. Soporte multiprotocolo

RADIUS no soporta los siguientes protocolos los cuales son soportados por TACACS+:

- Protocolo ARA (AppleTalk Remote Access)
- Net BIOS Frame Protocol Control protocol
- Interface de servicios asincronos de NOVELL
- Conexiones PAD X.25

e. Administración del router

RADIUS no permite a los usuarios controlar que comandos pueden ser ejecutados en un router y cuales no, por lo tanto, cuando se compara con TACACS+, RADIUS no es tan útil para el manejo de routers y no es tan flexible para los servicios de terminal.

f. Interoperabilidad

El estándar RADIUS no garantiza interoperabilidad, aunque muchos vendedores implementan los clientes RADIUS, esto no asegura que estos son ínter operables. Existen aproximadamente 45 atributos para RADIUS estándar. Usando los atributos

estándar se mejora la probabilidad de conseguir interoperabilidad. El uso de extensiones propietarias reduce la interoperabilidad.

g. AVP (Atribute-value pairs)

Cada AVP consiste de un tipo de identificador asociado con uno o más valores asignados. AVP esta especificado en un usuario o perfiles de grupos que define las características de autenticación y autorización para sus respectivos usuarios y grupos. TACACS+ y RADIUS implementan un arreglo de AVP cada uno separa los tipos de definiciones y características

Ejemplo de AVP para RADIUS	
Atributo	Tipo de valor
User-name	String
Password	String
Chap-Password	String
Client-id	Ip address
Login-host	Ip address
Login-service	Integer
Login-TCP-Port	Integer

Tabla 12.2 Ejemplo de AVP para Radius

Ejemplo de AVP para TACACS+	
Atributo	Tipo de valor
Inacl	Integer
Addr-poll	String
Addr	Ip address
Idletime	Integer
Protocol	Keyword
Timeout	Integer

Outacl	Integer

Tabla 12.3 Ejemplo de AVP para TACACS

12.5. CSACS.

El Servidor de Control de Acceso Seguro de Cisco (CSACS) para Windows provee una solución de identidad en la red centralizada y simplifica la experiencia del manejo de usuarios a través de todos los dispositivos y aplicaciones para la administración de seguridad de Cisco. El ACS de Cisco asegura la aplicación de las políticas asignadas al permitir a los administradores de red el controlar:

- Quien puede conectarse a la red
- Los privilegios que cada usuario tiene en la red
- Auditoria de seguridad grabada o información para el cobro mediante contabilidad.
- Control de comandos y acceso que están habilitadas para cada configuración del administrador.

CSACS en el pilar principal de las soluciones para seguridad de identidad y confianza en la red. Este extiende la seguridad de acceso al combinar autenticación, acceso de administrador y usuario, y control de políticas desde una estructura para la identidad en la red centralizada, permitiendo mayor flexibilidad y movilidad, la seguridad esta incrementada, así también la productividad de los usuarios.

Con CSACS se puede manejar y administrar acceso de los usuarios para los Routers, VPN, Firewalls, Conexiones de DSL, Dial up y Switches.

Las funciones avanzadas de CSACS son:

- Monitoreo de servicios automático, sincronización de la base de datos y importación de herramientas para despliegues a gran escala.

- Soporte para autenticación de usuarios de los siguientes servicios: LDAP (Lightweight Directory Access Protocol) y ODBC (Open Database Connectivity).
- Soporte para el tipo de autorización 802.1x flexible, incluyendo los siguientes protocolos: EAP-TLS (Extensible Autenticación Protocol Transport Layer Security), EAP (PEAP) protegido, Cisco LEAP, EAP-Flexible Authentication vía Secure Tunneling (EAP-FAST) y EAP-Message Digest Algorithm 5 (EAP-MD5)
- Una lista de control de acceso descargable para cualquier dispositivo de capa 3, incluyendo routers, Pix firewalls y VPN's de Cisco.
- Establecimiento de autorización para los comandos de los dispositivos.
- Restricciones de acceso a la red.
- Reporte de acceso administrativo y por usuario.
- Generación dinámica de cuotas.
- Restricciones de tiempo de acceso por ejemplo periodos de un día o días de la semana.
- Perfiles para usuario o grupo de dispositivos.
- Soporte para autenticación de VPN tradicionales y inalámbricas.
- Sincronización de base de datos externa.

CAPITULO 13. IMPLEMENTACIÓN DE UNA OPCIÓN DE SEGURIDAD APLICANDO DEFENSA EN PROFUNDIDAD.

En este capitulo se explica el esquema de seguridad que se va ha implementar, con cada uno de sus componentes, así como también la función que tiene cada uno de ellos y la razón por la cual forman parte del esquema de seguridad propuesto.

Para poder entender mejor lo que se pretende con el esquema de seguridad, se hará uso de un caso en el cual se plantea un problema que tiene una empresa hipotética y cada uno de los requerimientos de seguridad que necesita resolver, explicando específicamente con que elemento se soluciona cada problemática, de esta forma justificando así el porque se ha hecho uso de cada uno de ellos.

Nota: Debe de tomarse en cuenta que este esquema de seguridad no podría ser la mejor solución y se ha realizado de esta forma porque se tiene restricciones con el equipo disponible, por lo tanto se ha tratado de acomodar lo mejor posible.

13.1 PLANTEAMIENTO DEL PROBLEMA.

Cierta organización necesita implementar políticas de seguridad en sus redes internas para protegerse de ataques o uso indebido de información por parte de sus empleados, necesita también tener conexiones con sus sucursales para poder comunicarse con ellas de forma segura, además necesita proteger sus recursos del acceso público (Internet).

Los requerimientos generales corporativos son los siguientes:

- Implementar métodos de seguridad interna para proteger los recursos de la Intranet (Aplicaciones WEB, Bases de datos, Correo electrónico, FTP).
- Se necesita restringir el libre acceso a la red interna desde Internet.
- Se necesita algún tipo de protección antivirus.

- Los empleados y administradores en oficinas remotas necesitan ser autenticados.

La administración ha determinado los siguientes requerimientos específicos para los recursos en la oficina central.

- La comunicación de aplicaciones Web debe ser a través de VPN.
- El acceso a base de datos debe ser por medio de VPN.
- Para acceder al servicio de transferencia de archivos solamente será necesaria autenticación.
- Se debe de tener protección en contra de virus.
- En general se debe restringir el acceso indebido a la intranet.-

13.2 SOLUCIÓN.

Para la solución propuesta se han tomado recomendaciones proporcionadas por Cisco para el diseño e implementación de redes seguras, basándonos principalmente en el siguiente esquema.

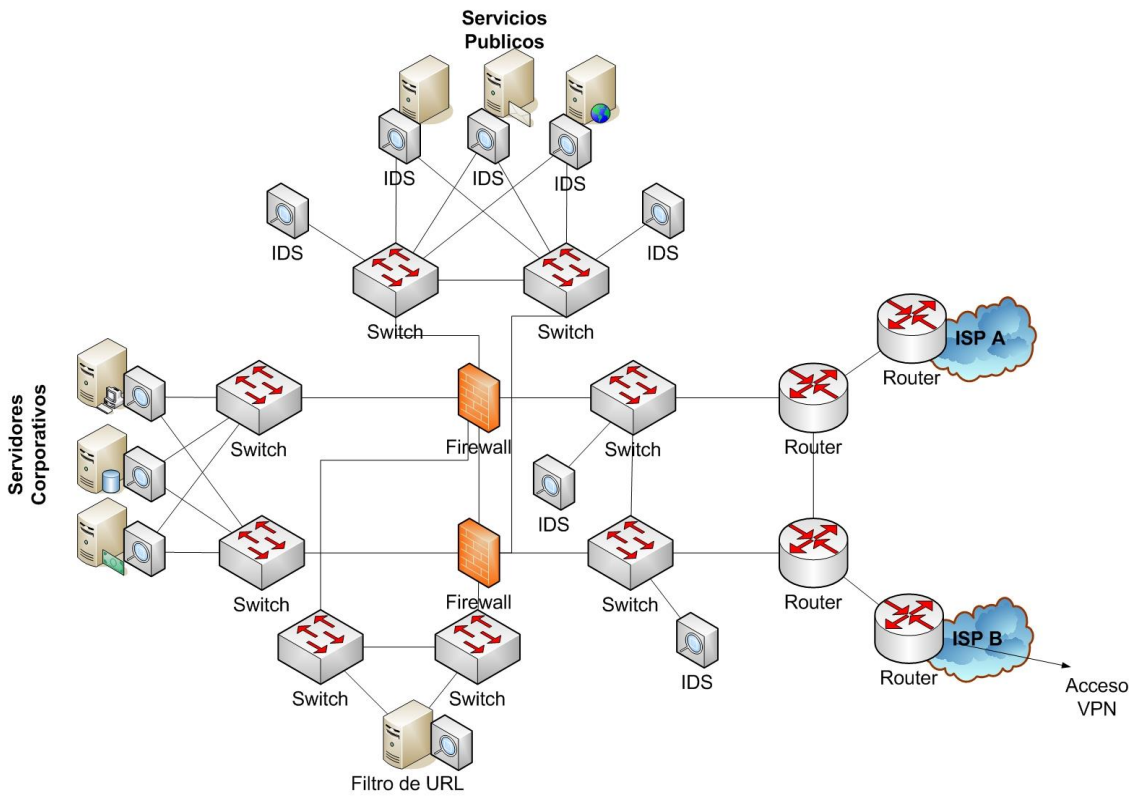


Figura 11.1. Esquema de red basado en la estrategia de seguridad Defensa en Profundidad.

Con este esquema se logran reducir las siguientes amenazas.

- Acceso no autorizado: se reducen a través del filtrado del ISP, el router del perímetro y el firewall corporativo.
- Ataques a nivel de la capa de aplicación: se reduce a través del IDS de host y de red.
- Ataques de virus y troyanos: se reduce a través del filtro del contenido del e-mail, host IDS y software antivirus.
- Ataques de contraseña: el sistema operativo y el IDS pueden detectar la amenaza.
- Negación de servicios: limitando la tasa de ruteo en ISP y controlando el flujo TCP SYN en el firewall.
- IP spoofing: filtros en el ISP y en el router del perímetro de la empresa.
- Paquetes sniffer: una infraestructura conmutada configurada apropiadamente y limitada por HIDS.

- Red de reconocimiento: Un IDS detecta reconocimientos; los protocolos son filtrados para limitar la efectividad.
- Explotación de la confianza: la VLAN restringe el modelo verdadero limitando los ataques basados en confianza.
- Redirección de puertos: el filtrado restringe y los HIPS limita los ataques.
- root kit, virus, gusanos: estos ataques son reducidos con HIPS y software antivirus.
- Acceso no autorizado a las URL (Bloqueo de contenidos): usado en conjunto con firewalls o Web proxy que bloquea las URL que han sido estimadas como no propias por las politicas de seguridad de la corporación.
- Ataques basados en URL: bloqueado con el uso de filtros URL en cargas balanceadas o caches de Web proxy.

13.2.1 Diseño Propuesto.

El diagrama que a continuación se describe esta basado en la figura 11.1.

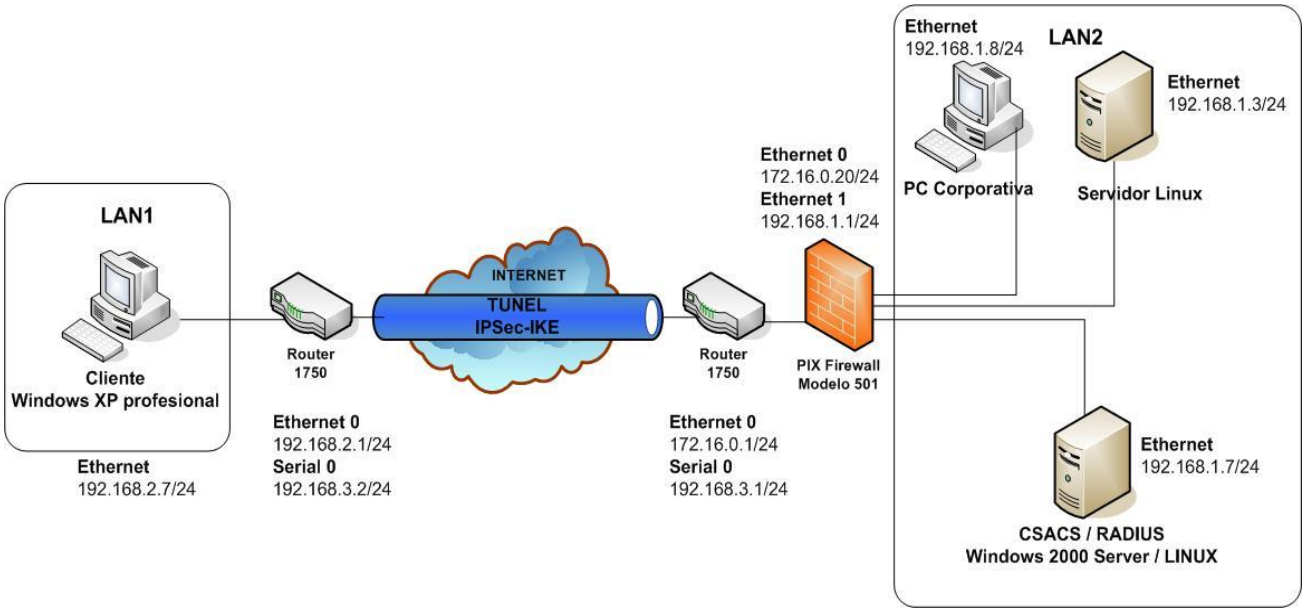


Figura 11.2 diagrama propuesto.

Definición en detalle de cada uno de los componentes que se utilizan.

El esquema de seguridad es la integración de varias tecnologías de protección las cuales en conjunto ofrecen mayor protección que cuando se utilizan de forma separada, a continuación se detalla cada uno de los dispositivos y tecnologías a utilizar para cubrir las necesidades del caso presentado.

13.2.2 La VPN.

Se utilizan dos Cisco Routers 1750 para establecer la comunicación entre la red corporativa y la sucursal.

Los objetivos son los siguientes:

a. Establecer comunicación entre ambos extremos.
b. Creación de un túnel virtual de comunicación entre ambos extremos.

Como se logran los objetivos:

Configurando los router para que se puedan comunicar entre ellos con tres opciones diferentes las cuales son:

- Protocolo RIP.
- Protocolo IGRP
- Protocolo EIGRP.

Y luego se configuran los router utilizando el protocolo de seguridad basado en IP llamado IPSec, a continuación se da detalle el proceso:

- El protocolo utilizado para el manejo del túnel virtual es:
  IPSec en modo túnel.

- El protocolo utilizado para la creación, negociación y establecimiento de los servicios que se utilizan en el túnel virtual es el siguiente: Protocolo IKE (Internet Key Exchange).
- Para llevar a cabo el cifrado de la información se utiliza el protocolo 3DES.
- El algoritmo que se utiliza para autenticar los datos de un paquete es: Algoritmo MD5 (Messages Digest 5).
- Establecimiento de llaves privadas y públicas.

a. Configuracion Protocolo RIP.

Con esta configuracion se logra que las interfaces Ethernet y serial del router cliente se comuniquen entre si y se comuniquen con el otro router en este caso con el router de perimetro el cual tambien.se configurara mas adelante con RIP

Router Cliente.

Habilitando la configuracion del protocolo de enrutamiento RIP

- **Cliente(config)# router rip**

Estableciendo redes de las interfaces que se necesitan que se comuniquen

Formato: network *direccion_de_red adyacente*

En este caso la direccion a utilizar es 192.168.2.0 que representa la red a la cual pertenece la direccion ip asignada a la interface Ethernet del router cliente.

- **Cliente(config-router)# network 192.168.2.0**

Luego se utiliza la direccion de red 192.168.3.0 que representa la red a la cual pertenece la direccion ip asignada a la interface Serial del router cliente.

- **Cliente (config-router)# network 192.168.3.0**

Router de Perimetro.

Habilitando la configuracion del protocolo de enrutamiento RIP

- **Perimetro(config)# router rip**

Estableciendo redes de las interfaces que se necesitan que se comuniquen

Formato: network *direccion_de_red adyacente*

En este caso la direccion a utilizar es 172.16.0.0 que representa la red a la cual pertenece la direccion ip asignada a la interface Ethernet del router de perimetro.

- **Perimetro (config-router)# network 172.16.0.0**

Luego se utiliza la direccion de red 192.168.3.0 que representa la red a la cual pertenece la direccion ip asignada a la interface Serial del router de perimetro.

- **Perimetro (config-router)# network 192.168.3.0**

Prueba de comunicación entre router cliente y router de perimetro.

Cliente# Ping 192.168.3.1

Perimetro# Ping 192.168.3.2

Nota: Para mayor información verificar el video **"Protocolo RIP en el Router Cliente"** en el anexo 2

Configuración de la vpn

Con esta configuración se logra que todo el tráfico originado en la red 192.168.2.0 y que tenga como destino la red 192.168.1.0 sea encriptado en el tunel de la VPN.

Router Cliente.

1. Configuración de ISAKMP
   - Habilitación de ISAKMP

     Cliente(config)# Crypto isakmp enable

   - Configuración de la política ISAKMP:

     Con este comando se define la politica que se va a configurar, a la cual se le asigna un número arbitrario, se debe de tomar en cuenta que el router toma como prioridad las politicas con menor número.

     Formato: crypto isakmp policy *numero_de_politica*

     Cliente(config)# Crypto isakmp policy 100

     - Algoritmo de encriptación

Aquí se define el algoritmo de encriptacion a utilizar por la politica establecida previamente. En este caso se utiliza el algoritmo 3Des

Formato: encryption *algoritmo_de_encriptacion*

Cliente(config-isakmp)# encryption 3des

- algoritmo hash

Aquí se define el algoritmo de hash a utilizar por la politica establecida previamente. En este caso se utiliza el algoritmo md5

Formato: hash *algoritmo_hash*

Cliente(config-isakmp)# hash md5

- método de autenticación

Se define el metodo de autenticacion para el intercambio de llaves

Formato: authentication *metodo_de autenticacion*

Cliente(config-isakmp)# authentication pre-share

- Método de cifrado de llaves

Se define el algoritmo a utillizar para llevar a cabo el cifrado de la llave precompartida.

Formato: group *numero_grupo*

Cliente(config-isakmp)# group 2

- Tiempo de vida

Se establece cada cuento tiempo se vuelve a generar el cifrado de llaves.

Formato: lifetime *tiempo_en_segundos*

Cliente(config-isakmp)# lifetime 10000

- Configuración de llave isakmp

  Especificación de la llave precompartida entre el router cliente y el router de perímetro

Formato: crypto isakmp key *llave_precompartida* address *direccion_ip_otro_router_vpn*

Cliente(config)# crypto isakmp key cisco1 address 192.168.3.1

2. Crear las listas de acceso crypto

   Se crea una lista de control de acceso que define que trafico se va a encriptar dentro del tunel VPN.

   Formato: access-list *numero_de_acl* deny | permit *tipo_de_protocolo direccion_origen direccion_destino*

   Cliente(config)# access-list 110 permit ip 192.168.2.0 0.0.0.255 172.16.0.0 0.0.0.255

3. Definir los conjuntos de transformaciones de datos

   Se define el conjunto de transformacion que va ser utilizado por ipsec.

   Formato: crypto ipsec transform-set *nombre_de_conjunto_transformacion combinacion_conjunto_de_transformaciones*

   Cliente(config)# crypto ipsec transform-set mivpn ah-md5-hmac esp-3des esp-md5-hmac

   - Definición del modo a utilizar

   Se establece el modo que va trabajar la VPN

   Formato: mode *tipo_de_tunel*

   Cliente (cfg-crypto-trans)# mode tunnel

4. Crear las entradas de crypto map

   Agrupacion de todos los componentes necesarios para el establecimiento de las asociaciones de seguridad IPSec

   Formato: crypto map nombre_del_mapa numero_de_secuencia ipsec_isakmp

   Cliente(config)# crypto map mivpn1 10 ipsec-isakmp

- Determinación del trafico que debe ser protegido por IPSec

  Formato: match address *id_lista_acceso*

  Cliente(config-crypto-map) # match address 110

- Especificación del conjunto de transformación utilizado por el crypto map

  Formato: set transform-set *nombre_de_conjunto_transformacion*

  Cliente (config-crypto-map)# set transform-set mivpn

- Especificación de otro router que utiliza la VPN

  Formato: set peer *nombre_host* | *direccion_ip*

  Cliente(config-crypto-map)#set peer 192.168.3.1

5. Aplicar las entradas de crypto map
   - Aplicando el crypto map a la interfaz serial 0

     Formato: crypto map *nombre_del_mapa*

     Cliente(config)# interface serial 0

     Cliente(config-if)# crypto map mivpn1

Nota: Para mayor información sobre la configuración de la VPN en el router cliente verificar el video **"Configuración VPN en el Router Cliente"** en el anexo 2

6. Monitorear y mantener IPSec
   - Comando para ver información acerca de la configuración IPSec

     Cliente # show crypto ipsec transform-set

     Cliente # show crypto map interface serial 0

     Cliente # show crypto isakmp sa
   - Ver el funcionamiento de la VPN

     Cliente#debug crypto ipsec

Cliente#debug crypto isakmp

Verificar la configuracion con los siguientes comandos

Muestra todas las configuraciones

show running-config

Muestra todas las interfaces que se han configurado y su estado

show ip interface brief

Verificar el funcionamiento de la vpn

para verificar el funcionamiento de la vpn primera mente se tienen que habilitar el IPSec y el IKE los comandos son los siguientes:

Debug crypto ipsec

Para mayor información buscar el video vpn debug en anexo dos

Debug cryto isakmp

Para mayor información buscar el video vpn debug en anexo dos

Router de perimetro.

Se debe de configurar igual que el router cliente

1. Configuración de ISAKMP

- Habilitación de ISAKMP

  Perimetro(config)# Crypto isakmp enable

- Configuración de la política ISAKMP:

Con este comando se define la politica que se va a configurar, a la cual se le asigna un número arbitrario, se debe de tomar en cuenta que el router toma como prioridad las politicas con menor número.

Formato: crypto isakmp policy *numero_de_politica*

Perimetro(config)# Crypto isakmp policy 100

- Algoritmo de encriptación

Aquí se define el algoritmo de encriptacion a utilizar por la politica establecida previamente. En este caso se utiliza el algoritmo 3Des

Formato: encryption *algoritmo_de_encriptacion*

Perimetro (config-isakmp)# encryption 3des

- algoritmo hash

Aquí se define el algoritmo de hash a utilizar por la politica establecida previamente. En este caso se utiliza el algoritmo md5

Formato: hash *algoritmo_hash*

Perimetro (config-isakmp)# hash md5

- método de autenticación

Se define el metodo de autenticacion para el intercambio de llaves

Formato: authentication *metodo_de autenticacion*

Perimetro (config-isakmp)# authentication pre-share

- Método de cifrado de llaves

Se define el algoritmo a utillizar para llevar a cabo el cifrado de la llave precompartida.

Formato: group *numero_grupo*

Perimetro (config-isakmp)# group 2

- Tiempo de vida

Se establece cada cuento tiempo se vuelve a generar el cifrado de llaves.

Formato: lifetime *tiempo_en_segundos*

Perimetro (config-isakmp)# lifetime 10000

- Configuración de llave isakmp

Especificación de la llave precompartida entre el router cliente y el router de perímetro

Formato: crypto isakmp key *llave_precompartida* address *direccion_ip_otro_router_vpn*

Perimetro (config)# crypto isakmp key cisco1 address 192.168.3.2

2. Crear las listas de acceso crypto

Se crea una lista de control de acceso que define que trafico se va a encriptar dentro del tunel VPN.

Formato: access-list *numero_de_acl* deny | permit *tipo_de_protocolo direccion_origen direccion_destino*

Perimetro (config)# access-list 110 permit ip 172.16.0.0 0.0.0.255 192.168.2.0 0.0.0.255

3. Definir los conjuntos de transformaciones de datos

Se define el conjunto de transformacion que va ser utilizado por ipsec.

Formato: crypto ipsec transform-set *nombre_de_conjunto_transformacion combinacion_conjunto_de_transformaciones*

Perimetro (config)# crypto ipsec transform-set mivpn ah-md5-hmac esp-3des esp-md5-hmac

- Definición del modo a utilizar

Se establece el modo que va trabajar la VPN

Formato: mode *tipo_de_tunel*

Perimetro (cfg-crypto-trans)# mode tunnel

4. Crear las entradas de crypto map

Agrupacion de todos los componentes necesarios para el establecimiento de las asociaciones de seguridad IPSec

Formato: crypto map nombre_del_mapa numero_de_secuencia ipsec_isakmp

Perimetro (config)# crypto map mivpn1 10 ipsec-isakmp

- Determinación del trafico que debe ser protegido por IPSec

  Formato: match address *id_lista_acceso*

  Perimetro (config-crypto-map) # match address 110

- Especificación del conjunto de transformación utilizado por el crypto map

  Formato: set transform-set *nombre_de_conjunto_transformacion*

  Perimetro(config-crypto-map)# set transform-set mivpn

- Especificación de otro router que utiliza la VPN

  Formato: set peer *nombre_host* | *direccion_ip*

  Perimetro (config-crypto-map)#set peer 192.168.3.2

5. Aplicar las entradas de crypto map
   - Aplicando el crypto map a la interfaz serial 0

     Formato: crypto map *nombre_del_mapa*

     Perimetro (config)# interface serial 0

     Perimetro(config-if)# crypto map mivpn1

6. Monitorear y mantener IPSec
   - Comando para ver información acerca de la configuración IPSec

     Perimetro # show crypto ipsec transform-set

     Perimetro # show crypto map interface serial 0

     Perimetro # show crypto isakmp sa

   - Ver el funcionamiento de la VPN

     Perimetro #debug crypto ipsec

     Perimetro #debug crypto isakmp

Nota: Para mayor información verificar el video **“Probando la VPN”** en el anexo 2

13.2.3. Restringir el acceso general a la red interna.

Es necesario establecer políticas de seguridad el cual nos ayudan a prevenir de personas que desean ocasionar problemas dentro de la red.

El objetivo es el siguiente:

a. Se necesita restringir el acceso público a la red interna.

Como se logra este objetivo:

Los router se configuran utilizando Listas de Control de Acceso y se configura un pix firewall. Ademas se configura un servidor de autenticación, autorización y contabilidad para restringir el acceso a los servicios de la red corporativa.

A continuación se detalla como se a configurado al pix firewall

a. Configuración del Pix Firewall:

1. Configuración de las direcciones IP de las interfaces del pix firewall:
   Formato: ip address *nombre_interface direccion_ip mascara_subred*

   a. Interfaz outside:
      - Pix (config)# ip address outside 172.16.0.20 255.255.255.0

   b. Interfaz inside:
      - Pix (config)# ip address inside 192.168.1.1 255.255.255.0

2. Configuracion de la ruta estatica para la interfaz outside:

Se especifica la direccion IP de salida para la red interna.

Formato: route *nombre_interface direccion_ip mascara_subred direccion_ip_router_outside metrica*

- Pix (config)# route outside 0 0 172.16.0.1 1

3. Configuracion de NAT:

   Se establece la protecció de las direcciones IP de la red interna hacia la red externa

   Formato: nat *numero_identicacion_nat direccion_ip_local mascara_subred*

   - Pix (config) # nat (inside) 10 192.168.1.0 255.255.255.0

4. Configuracion de Global:

   Se establece la protección de la direcciones IP de la red interna mediante el uso de una direccion IP de salida especifica.

   Formato: global *numero_identificacion_nat direccion_ip_outside_salida*

   - Pix (config) # global (outside) 10 172.16.0.21

5. Configuracion de Static:

   Configuración de la comunicación fija entre la direccion ip outside y la direccion ip de host interno.

   Formato: static *direccion_ip_outside direccion_ip_host_red_interna*

Configuración del pix firewall para restringir el acceso a puertos específicos hacia la red corporativa:

Para el tráfico http entrante :

- Pix (config) # Static (inside,outside) tcp 172.16.0.20 80 192.168.1.3 80 netmask 255.255.255.255 0 0

Para el tráfico ftp entrante :

- Pix (config) # Static (inside,outside) tcp 172.16.0.20 21 192.168.1.3 21 netmask 255.255.255.255 0 0

Para el tráfico telnet entrante :

- Pix (config) # Static (inside,outside) tcp 172.16.0.20 telnet 192.168.1.3 telnet netmask 255.255.255.255 0 0

6. Configuracion de la lista de acceso :
   Establecimiento del trafico permitido entre la red externa y la interface outside del pix firewall:

   Tambien se puede lograr el acceso restringido a puertos que el pix firewall puede utilizar mediante el uso de listas de acceso con los puertos permitidos por la red corporativa:

   Formato: access-list *nombre_lista_acceso* permit | deny *protocolo direccion_origen mascara_subred direccion_destino mascara_subred*

   - Pix (config)# access-list acl_in permit tcp host 192.168.2.7 host 172.16.0.20 eq http
   - Pix (config)# access-list acl_in permit tcp host 192.168.2.7 host 172.16.0.20 eq ftp
   - Pix (config)# access-list acl_in permit tcp host 192.168.2.7 host 172.16.0.20 eq telnet
   - Pix (config)# access-list acl_in permit icmp any any

7. Configuracion del grupo de acceso :
   Establecimiento de la lista de acceso a la interface outside:
   Formato: access-group *numbre_lista_acceso* in interface *nombre_interface*

   - Pix (config)# access-group acl_in in interface outside

Nota: Para mayor información verificar el video **"Configuración de Interfaces Pix FIrewall"** en el anexo 2

b. Configuracion de los servicios AAA en el PIX Firewall:

Para efectos de demostración se ha configurado el pix firewall de manera que cada cierto tiempo se realice la autenticación del usuario cuando desea acceder a cualquiera de los servicios que ofrecen (http, ftp, telnet, etc), con el propósito de ofrecer una mayor seguridad a la información de la red corporativa ya que si un usuario es descuidado y por algún motivo tiene que ausentarse del puesto de trabajo o se le olvida que ya realizo este procedimiento y no deja la computadora debidamente asegurada (bloqueada contra el acceso no autorizado), una vez ya autenticado, los datos quedan a disposición de cualquier persona, y si esto es aprovechado por terceras personas ajenas a la corporación la confidencialidad de los datos estaría comprometida.

Por tal razón, la autenticación es llevada a cabo cada cierto periodo de tiempo, con el propósito de asegurar que los datos van a ser accesados solamente por usuarios auténticos y que tiene autorización para acceder a esta información ya que si esta persona quiere acceder a mas información o desea acceder a otro servicio tiene que realizar la autenticación del mismo otra vez para verificar que en realidad es quien dice ser y que tiene derecho a acceder a esa información.

Por defecto, la autenticación del usuario se lleva a cabo una sola vez, ya autenticado el usuario, este puede acceder a todos los datos que esta autorizado. Este acceso a los datos dura hasta que el usuario se desconecta de la red corporativa o reinicia la computadora.

1. Especificación del servidor AAA:

Especificacion del protocolo a utilizar y el servidor que ofrece los servicios AAA:

Protocolo AAA a utilizar:

Formato: aaa-server *nombre_grupo_AAA protocolo_AAA_a_utilizar*

Servidor AAA a utilizar:

Formato aaa-server *nombre_grupo_AAA* host *direccion_ip_servidor_AAA llave_secreta_AAA*

- Pix (config) # aaa-server mitacacs+ tacacs+
- Pix (config) # aaa-server mitacacs+ host 192.168.1.7 keyra

2. Habilitacion de la autenticación de servicios:

   Configuracion de la autenticación de los usuarios externos que intentan acceder a los servicios ofrecidos por la red interna

   Formato: aaa authentication include *servicio_a_autenticar nombre_interface direccion_ip_local mascara_subred direccion_ip_externa mascara_subred nombre_grupo_AAA*

   - Servicio de Telnet:
     - Pix (config)# aaa authentication include telnet outside 0 0 0 0 mitacacs+
   - Servicio de Http:
     - Pix (config)# aaa authentication include http outside 0 0 0 0 mitacacs+
   - Servicio de Ftp:
     - Pix (config)# aaa authentication include ftp outside 0 0 0 0 mitacacs+

3. Habilitacion de la autorización de servicios:

   Configuracion de la autorización de los usuarios externos para conocer a que servicios ofrecidos por la red interna tiened acceso.

   Formato: aaa authorization include *servicio_a_autorizar nombre_interface direccion_ip_local mascara_subred direccion_ip_externa mascara_subred nombre_grupo_AAA*

   - Servicio de Telnet:
     - Pix (config)# aaa authorization include telnet outside 0 0 0 0 mitacacs+

- Servicio de Http:
    - Pix (config)# aaa authorization include http outside 0 0 0 0 mitacacs+
- Servicio de Ftp:
    - Pix (config)# aaa authorization include ftp outside 0 0 0 0 mitacacs+

4. Habilitacion de la contabilidad de servicios:

Configuracion de la contabilidad de los usuarios externos sobre los servicios que han sido accesados y utilizados.
Formato: aaa accounting include *servicio_a_contabilizar nombre_interface direccion_ip_local mascara_subred direccion_ip_externa mascara_subred nombre_grupo_AAA*

- Servicio de Telnet:
    - Pix (config)# aaa accounting include telnet outside 0 0 0 0 mitacacs+
- Servicio de Http:
    - Pix (config)# aaa accounting include http outside 0 0 0 0 mitacacs+
- Servicio de Ftp:
    - Pix (config)# aaa accounting include ftp outside 0 0 0 0 mitacacs+

Nota: Para mayor información sobre la configuracion del los servicios AAA verificar el video **"Configuración de AAA en el Pix FIrewall"** en el anexo 2

5. Configuración de los mensajes a desplegar para los servicios AAA :

Se personalizan los mensajes que son desplegados por las diferentes ventanas utilizadas por el servidor AAA.

- Configuración del mensaje principal:
  Formato: auth-prompt prompt *mensaje_a_desplegar*

  - Pix (config)# auth-prompt prompt Por favor introduzca su usuario y password para ingresar al SERVIDOR TESIS

- Configuración del mensaje de aceptacion:
  Formato: auth-prompt accept *mensaje_a_desplegar*

  - Pix (config)# auth-prompt accept Autenticacion exitosa al SERVIDOR TESIS

- Configuración del mensaje de error
  Formato: auth-prompt reject *mensaje_a_desplegar*

  - Pix (config)# auth-prompt reject ERROR de autenticacion , Acceso Denegado al SERVIDOR TESIS

Nota: Para mayor información verificar el video **"Probando control de acceso en el Pix Firewall"** en el anexo 2

c. El CSACS.

Requerimientos para ejecutar CSACS

- Software:
  - Microsoft Internet Explorer 6.0
  - Netscape Communnicator 6.2
  - Windows 2000 Server con Service Pack 1 o 2 instalado.

- Hardware:
    - Procesador Pentium III o superior corriendo a 550 MHz o superior
    - 250 MB de espacio libre en el disco duro
    - 256 MB de memoria RAM
    - Resolución de pantalla mínima de 800x600 utilizando 256 colores.

Funcionamiento del AAA

1. El cliente requiere conexión con los recursos de la red corporativa, en este tramo la información se envía vulnerable.
2. Se encripta con IPSec la información de conexión a los recursos.
3. El cliente AAA (PIX Firewall) recibe la petición de acceso a los recursos y este le pide al cliente el nombre de usuario y password.
4. Se encripta con ipSec la información de petición de usuario y password que realizo el cliente AAA.
5. El cliente envía la informaron de usuario y password al cliente AAA
6. Se encripta con IPSec la información enviada por el cliente hacia el cliente AAA.
7. El cliente AAA envía información del cliente al CSACS.
8. El CSACS envía al cliente AAA una respuesta de acceso permitido o denegado para acceder a los recursos de la red.
9. El cliente AAA envía la respuesta obtenida del CSACS al cliente.
10. Se encripta la respuesta del Cliente AAA con IPSec.
11. Si el acceso del cliente es permitido entonces puede acceder a los recursos de la red corporativa.

13.2.4 Protección de Virus.

Se utiliza como esquema de protección contra virus la utilización de software antivirus.

El objetivo es el siguientes:

a. Proteger de virus a cada computadora de la intranet. Es necesario proteger en contra de virus ya que estos pueden permitir el acceso a una red protegida, además de que pueden causar perdidas de información.

Como se logra este objetivo:

Instalando un software antivirus en cada computadora individual que forma parte de la red interna.

- El Software a utilizar para la protección en contra de virus es el siguiente: Norton Enterprise.

13.2.5 Implementación de los recursos corporativos.

Se utiliza una computadora en la cual se instala y configura cada uno de los recursos especificados.

Los objetivos son los siguientes:

a. Proporcionar los recursos que están disponibles en la red corporativa.
b. Se requiere implementar servicios generales tales como: Web, Telnet, FTP, Base de Datos y Mail.

Como se logra este objetivo:

Instalando el sistema operativo Linux con los siguientes servicios habilitados y configurados debidamente para su funcionamiento.

- El servidor Web utilizado es: Apache.
- El servidor de Base de Datos : My SQL
- El servidor de transferencia de archivos (FTP): Very Secure FTP Server (vsftpd)
- Correo: Send Mail

- Conexiones Telnet

13.2.6. Configuración de la computadora que representa al cliente en la oficina remota.

Se utiliza una computadora la cual necesita acceder a los recursos ofrecidos por la oficina central o red corporativa.

Los objetivos son los siguientes:

a. Permitir el acceso de forma segura a los recursos de la red corporativa.
b. Se necesita que se establezca una comunicación ente cliente y la red corporativa y además no se comprometa la información que se maneja dentro de esta.

Como se logra este objetivo:

Configurando la computadora cliente para que pueda acceder a los recursos de la red corporativa y la comunicación sea segura.

La configuración de la computadora cliente es la siguiente:

- Sistema Operativo utilizado: Windows XP
- Antivirus utilizado Norton Corporate.

RECOMENDACIONES

Para contar con un sistema de información que sea seguro es preciso cambiar la perspectiva que se tiene del mismo, y comenzar a considerarlo como un proceso mas dentro de la organización.

Existen varias recomendaciones que pueden ayudar a la hora de iniciar esta trayectoria entre las que destacaríamos las siguientes:

Apreciación general del ambiente de control

- Tener siempre en la mente el tema de la seguridad, hasta que sea algo relativo a la naturaleza de un ser.

- Apoyo visible y compromiso por parte de la dirección de la organización.

- Normativa de seguridad, objetivos y actividades que reflejan los objetivos del negocio.

- Enfoque para la implantación de medidas de seguridad coherentes con la política de la organización.

- Desarrolle un plan corporativo de respuesta ante incidentes de seguridad.

- Disponer de un documento integral de Políticas de seguridad de la red.

- Buen entendimiento de los requisitos de seguridad, evaluación y gestión de riesgos.

- Garantizar que se cumplan con la política de seguridad en cada departamento

- Prueba periódicamente de la red corporativa en busca de vulnerabilidades.

- Sistema de medición exhaustivo y equilibrado para evaluar la gestión de la seguridad de la información, del cual se obtengan sugerencias para realizar mejoras.

Adecuación a las normas generales de seguridad informática

- Utilizar procedimientos formales de administración de usuarios y un adecuado mantenimiento.

- Asignar las responsabilidades sobre seguridad de la información

- Facilitar la formación y educación apropiada para formar a los empleados en seguridad de la información

- Disponer de los canales necesarios para que el personal pueda comunicar las incidencias de seguridad

- Fortalecer los controles en materia de prevención de incendios.

- Elaborar un plan de contingencias y recuperación de desastres, realizar pruebas, documentarlas, evaluar los resultados, mantenerlo actualizado y guardar una copia del mismo en un sitio seguro y externo.

Seguridad del Hardware y Software

- Acotar la responsabilidad de administración de seguridad con la creación de la función del Administrador de Seguridad.

- Elaborar una lista de controles estándares que deberán tener los sistemas.

- Implementar medidas que controlen y alerten las posibles evasiones a controles de seguridad.

- Monitorear periódicamente los registros de auditoria de los sistemas y verificar que sólo se realizan modificaciones debidamente autorizadas a los datos críticos.

- Realice periódicamente copias de seguridad de los datos de mayor importancia en la organización.

- Guardar los respaldos de documentación, programas, ejecutables y datos de los sistemas, copias actualizadas y de toda documentación crítica o sensible en un sitio seguro externo.

- Compruebe periódicamente el nivel de seguridad con el que estas conectado por ejemplo: scan de puertos, antivirus, firewall, datos sensibles en la configuración de cuentas.

- Instale las actualizaciones y parches necesarios en las PC para controlar la mayor cantidad de vulnerabilidades conocidas.

- Regularmente actualice el software de las PC que forman parte de la organización con las últimas versiones.

- Tener en cuenta un antivirus y mantenerlo siempre actualizado.

- No mantenga puertos innecesarios abiertos, ni servicios o aplicaciones corriendo que no se utilizan.

- Controle permanentemente sus mecanismos de defensa

Manejo de Claves Secretas o Passwords

- Utilizar claves secretas diferentes en todos los servicios que utilice, como por ejemplo la de su correo electrónico.

- No utilice claves que sean fácilmente identificables como fechas de nacimiento, teléfonos, direcciones, o nombres de familiares.

- Requiera el uso de claves que contengan combinaciones de caracteres alfanuméricos especiales

- No revele por ningún motivo las claves secretas

- No anote las claves, memorícelas.

- Ingrese su clave de manera confidencial de forma que no pueda ser vista por otras personas que están a su alrededor.

- Obligue a sus usuarios al cambio periódico de claves de acceso.

- Cancele todas las claves de acceso de empleados que dejen la empresa por cualquier motivo

Correo electrónico.

- Desconfíe de los correos que pidan información personal o financiera como nombres de usuario y contraseñas, números de tarjetas de crédito, y otra información privilegiada, especialmente de aquellos cuyo tono sea alarmista.

- Evite abrir cualquier archivo adjunto de un email sospechoso, ya que puede ejecutar un programa de código malicioso para robar información personal.

- Considere la instalación de software de seguridad, como el ofrecido por empresas de alto prestigio en seguridad informática, que pueden ayudar a detectar programas maliciosos (antivirus), filtrar spam (filtros de spam) y/o asegurar el uso de Internet seguro (cortafuegos). Estos programas pueden ayudar a prevenir daños en su sistema y le protegerán de ataques de hackers y estafadores

Tecnología.

Las empresas para poder comunicarse necesitan optar por tecnologías avanzada y que son útiles para mitigar los ataques las tecnologías que recomendamos son las siguientes:

- Es recomendable establecer las políticas de seguridad de cada equipo así como también las políticas ante cualquier desastre natural o desastre del entorno.

- Utilizar tecnología VPN para asegurar que los datos viajen de una forma segura.

- Es recomendable utilizar el manejo de llaves compartidas que proporcionan el protocolo IKE y sus respectivos algoritmos de encriptamiento como lo son 3Des, des.

- En las configuraciones de los router y en los firewall utilizar listas de acceso.

- Utilizar NAT para ocultar las verdaderas ip.

- Es muy útil un firewall ya que nos protege de distintos ataques.

- Para llevar el nivel de seguridad mas alto es necesario configurar un servidor de autenticación, autorización y así permitir el ingreso a la red a usuarios debidamente registrados.

- Una estrategia para asegurar la red contra virus es utilizar tecnología Systematic aunque existen otras.

- Es recomendable utilizar servidores linux ya que son: confiables, y debajo para proveer servicios de una forma eficiente y efectiva.

- Los servicios proporcionadas por la organización deben estar debidamente configurados para evitar posibles vulnerabilidades.

- Es necesario estar monitoriando la red o los servicios de una forma constante con herramientas adecuadas para este fin.

- Los administradores de red deben estar constantemente actualizando el equipo y haciendo mejoras a la seguridad de red. Ya que las tecnologías están en constante cambio.

- Es recomendable utilizar tecnología como: IDS e IPS para agregar un nivel mas a la pirámide de seguridad.

- Es recomendable que los administradores de red estén constantemente en cursos y capacitaciones para poder hacer frente a los desafíos de seguridad.

CONCLUSIONES

- Seguridad = confiabilidad + Integridad + Disponibilidad.
- La seguridad debe ser gestionada y medida de forma adecuada, mejorando continuamente los niveles alcanzados.

- La seguridad es un factor clave en las redes de datos seguras. La protección de la disponibilidad de las redes de datos es uno de los principales retos actuales. Los fabricantes de equipos están esperando incluir un creciente conjunto de facilidades para mitigar los efectos de los ataques. Este activo campo de investigación está produciendo un grupo de tecnologías que está madurando en soluciones adecuadas comerciales.

- Los mecanismos de ataques y sus homólogos defensivos por lo general evolucionan en paralelo, la calidad de los programas tiene potencial para reducir considerablemente la exposición de las redes de datos

- Es importante hacer notar que siempre existirá una lucha entre la tecnología de seguridad que se puede desplegar y la privacidad y transparencia de las redes de datos que son la base de su éxito.

- Se tiene una mayor conciencia de los aspectos técnicos del problema, pero no existe una cultura de la seguridad a nivel empresarial que haga que la dirección plantee otros tipos de medidas más haya de las técnicas.

- En efecto, aunque existan diversas tendencias, la situación final esta mucho más clara. Existen pequeñas variaciones temporales o locales. Lo cierto es que existe una visión generalizada de hacia donde se dirige la Sociedad de la Información (SI), compartida en todo el mundo. Defensa en seguridad

- En general las organizaciones tratan de solventar la problemática de la seguridad mediante la implantación de productos, tratando de evitar en la

medida de lo posible la adopción de medidas de tipo administrativo o de gestión en general.

- En la sociedad del futuro la información será el activo y la fuente de riqueza más importante. Por lo tanto, serán las empresas las que lideren la iniciativa para la introducción de las nuevas tecnologías, puesto que serán las principales beneficiarias de la misma. Las empresas no pueden concebirse sin acceso a Internet y sin hacer uso de todas las posibilidades que ofrece: acceso y difusión de información a clientes, proveedores y empleados, compra y venta online, gestión interna de la empresa, etc., todo ello con el gran valor añadido de la independencia geográfica de cada uno de los agentes. Esta integración con la Sociedad de la Información conllevará importantes cambios, sobre todo en la forma de organizarse y en los procesos internos.

- Los usuarios y los ciudadanos van a ser los beneficiarios últimos de las nuevas tecnologías. Sin embargo, el proceso de adopción de las nuevas soluciones en el ámbito de seguridad es lento. Inicialmente, la introducción de estas nuevas tecnologías se realiza a través del mundo empresarial.

- En el futuro existirá mayor acceso a la educación acerca de seguridad en redes. Sin embargo, para que llegue la información a todos será preciso reducir el costo de la información, aumentar su calidad, y sobre todo, que existan contenidos interactivos atractivos.

- Hoy en día las empresas todavía se encuentran en cambios acerca de la seguridad. Las PYMES no se encuentran en capacidad de pagar grandes sumas de dinero para implementar un esquema de seguridad.

- Aunque se tengan todos los libros acerca de configuraciónes es necesario entender el procedimeinento que se debe seguir , que es lo que se desea hacer y comprender para que se utiliza cada comando en las configuraciones y asi de esta manera se va poder aplicar a lo que se desea realizar.

- Un aspecto esencial será convencer a los empleados y a los propios directivos de que el uso de nuevas tecnologías es beneficiosa y que, por lo tanto, cualquier inversión en educación y formación siempre será rentable.

- Los temas relacionados con el personal son especialmente delicados, siendo las organizaciones reacias a adoptar cualquier tipo de medida que afecte al personal. Es fundamental entender que no se puede lograr un nivel de seguridad razonable sin implicar al personal de la empresa en el proceso

- Hoy en día es necesario que el usuario y el ciudadano comience a familiarizarse con las nuevas tecnologías así como también las personas encargadas de mantener segura la información y los servicios que ofrece dicha organización.

- Defensa en profundidad es una estrategia de seguridad de redes que muchas organizaciones y empresas están utilizando ya que disminuyen el riesgo de ser atacados por intrusos o personas mal intencionadas.

- Las VPNs son tecnologías que pueden ser utilizadas por las organizaciones para poder comunicarse de una manera segura por una rede insegura ya que aplica a los datos diferentes algoritmos de encriptación, autenticación.

- Una de las mejores maneras de tener a los usuarios debidamente registrados, autorizados y monitoriados es utilizando un servidor de autenticación autorización y contabilidad comúnmente conocido como: AAA.

- Los firewall son una tecnología que protegen de la mayoría de ataques y nos permite mantener nuestra red segura, libre de intrusos y de personas no autorizadas.

- Las estrategias contra virus en una organización son muy importantes. Las estadísticas mencionadas en él capitulo dos muestran que la mayoría de ataques son producto de algún virus. Es necesario que las organizaciones tengan sus antivirus actualizados.

- Aunque existan muchos mecanismos de seguridad o estrategias de seguridad no va ha estar cien por cinto segura su red.

FUENTES DE INFORMACION.

A continuación se menciona el material consultado para la elaboración de la tesis.

BIBLIOGRAFÍAS:

- **VPN: A Beginner's Guide**
  John Mairs
  Osborne/McGraw-Hill
  Primera Edición, 2001
- **IPSec: Securing VPNs**
  Carlton Davis
  Osborne/McGraw-Hill.
  2001
- **IPSec VPN Design**
  Vijay Bollapragada, Mohamed Khalid, Scott Wainner
  Cisco Press
  2005
- **Virtual Private Networks: Technologies and Solutions**
  Ruixi Yuan, W. Timothy Strayer
  Addison-Wesley Professional
  Primera edicion 2001
- **Layer 2 VPN Architectures (Networking Technology)**
  Wei Luo, Carlos Pignataro, Anthony YH Chan, Dmitry Bokotey
  Cisco Press
  2005
- **Troubleshooting Virtual Private Networks (VPN)**
  Mark Lewis
  Cisco Press
  2004
- **Cisco Router Firewall Security**
  Richard Deal
  Cisco Press

2004

- **Cisco Field Manual: Router Configuration**
  David Hucaby, Stephen McQuerry, Steve McQuerry
  Cisco Press
  Primera edicion 2001
- **Network Security Architectures**
  Sean Convery
  Cisco Press
  2004
- **Hardening Cisco Routers**
  Thomas Akin
  O'Reilly
  Primera edicion 2002
- **Cryptography Protocols and Algorithms**
  Skillsoft press
  2003
- **Secure PIX and Secure VPN Study Guide**
  Wade Edwards
  Sybex,
  2003
- **IP Routing Fundamentals**
  Mark A. Sportack
  Cisco Press
  2001
- **Building a Virtual Private Network**
  Meeta Gupta
  Premier Press
  2003.
- **CISCO ACCESS CONTROL SECURITY: AAA Administration Services**
  Brando J. Carroll
  Cisco Press

Primera edición 2004.

- **SETTING UP A VPN**
  Rajiv Charles
  SkillSoft Corporation
  Primera edición 2002.
- **CISCO SECURE PIX FIREWALL FUNDAMENTALS**
  Cisco Press
  2000.
- **CISCO ROUTER FIREWALL SECURITY**,
  Richard A. Deal
  Cisco Press
  2004.
- **Web Security Basics**
  Shweta Bhasin
  Premier Press
  2003
- **Security Architecture: Design Deployment and Operations**
  Christopher M. King, Curtis E. Dalton y T. Ertem Osmanoglu
  McGraw-Hill/Osborne
  2001
- **Rethinking Public Key Infrastructure and Digital Certificates**
  Stefan A. Brands
  The MIT Press
  2000

SITIOS WEB:

- www.cisco.com proveedor de productos y servicios de seguridad. Estados Unidos.
- www.cisco.com/univercd/cc/td/doc/cisintwk/index.htm,CISCO SYSTEMS. Soluciones para el transporte de datos, voz y video integrados. Argentina. Enero 2005.
- www.monografias.com, MONOGRAFIAS. Recursos Educativos en la Red, Argentina. Enero 2005
- www.rfc-editor.org/rfc/rfc1058.txt, The Request for Comments Editor. Publicación de notas técnicas del Internet. Estados Unidos. Agosto 2005.
- www.microsoft.com, Microsoft. Facilitar a las personas y empresas el desarrollo profesional a través de la tecnología. Estados Unidos. Enero 2005.
- www.xtech.com.ar, XTECH. Desarrollo de aplicaciones, productos, servicios y soporte para empresas y organizaciones que deseen disfrutar de los beneficios del mejor sistema operativo LINUX, Argentina. Diciembre 2004
- www.vpnc.org. VIRTUAL PRIVATE NETWORK CONSORTIUM, Promover los productos de nuestros miembros a la prensa así como a potenciales clientes. Estados Unidos. Julio 2004.
- http://www.vmyths.com/. Últimas noticias y base de datos sobre las verdades y mentiras alrededor de los virus informáticos. Estados Unidos. Marzo 2005.
- https://www.icsalabs.com/. Estándares y certificaciones para productos comerciales en seguridad. Estados Unidos. marzo 2005.
- http://www.sans.org/. SANS es la fuente confiada para implementar medidas de seguridad de información y certificación en el mundo. Estados Unidos. Abril 2005.
- http://www.nsa.gov/home_html.cfm. Coordina, dirige, y realiza actividades altamente especializadas para proteger sistemas de información del gobierno de ESTADOS UNIDOS. Abril 2005.
- http://www.rfc-es.org/. traducción al español de la documentación estándar sobre Internet conocida como RFC (Request For Comments). En esta serie de

documentos se detalla prácticamente todo lo relacionado con la tecnología de la que se sirve Internet: protocolos, recomendaciones, comunicaciones.

- http://www.pandasoftware.es/. Proveedor de software antivirus. Abril 2005.
- http://www.symantec.com/index.htm. Proveedor de software antivirus. Abril 2005.
- http://www.mcafee.com/us/. Proveedor de software antivirus. Abril 2005.
- http://www.defenselink.mil/. Web site oficial para el departamento de la defensa y del punto de partida para encontrar la información acerca de seguridad de los Estados Unidos en línea. Abril 2005.
- http://alerta-antivirus.red.es/seguridad/ver_pag.html?tema=S&articulo=4&pagina=1. Centro de alerta temprana sobre virus y seguridad informática. Mayo 2005.
- http://www.cert.org/. Instituto de la seguridad de la computadora (CSI) es la organización principal del mundo dedicada específicamente a proporcionar información acerca de las computadoras y seguridad de la redes. Estados Unidos. Mayo 2005.
- http://www.gocsi.com/. El instituto de la seguridad de la computadora (CSI) es la organización principal del mundo dedicada específicamente a porción información, de la seguridad en las computadoras y la seguridad de la red. Mayo 2005.
- http://www.securityfocus.com/. SecurityFocus es un sitio de información de seguridad confiable y comprensiva. Estados unidos. Mayo 2005
- http://www.net-security.org/. Net-security es un portal de información acerca de seguridad administrable de una manera privada. Estados Unidos. Mayo 2005
- http://csrc.nist.gov/. Instituto de estandarización de tecnologías. Estados Unidos. Mayo 2005
- http://www.sec.gov/. Comisión de intercambio de seguridad de los Estados Unidos. Mayo 2005.

GLOSARIO.

A

ACL (lista de control de acceso): Lista mantenida por un router de Cisco para controlar el acceso desde o hacia un router para varios servicios (por ejemplo, para evitar que los paquetes con una dirección IP determinada salgan de una interfaz en particular del router).

Actualización del enrutamiento: Mensaje que se envía desde el router para indicar si la red es accesible y la información de costo asociada. Normalmente, las actualizaciones del enrutamiento se envían a intervalos regulares y luego de que se produce un cambio en la topología de la red. Comparar con actualización relámpago.

Administración de red: Uso de sistemas o acciones para mantener, caracterizar o realizar el diagnóstico de fallas de una red.

Administrador de red: Persona a cargo de la operación, mantenimiento y administración de una red.

Aplicación: Programa que ejecuta una función directamente para un usuario. Los clientes FTP y Telnet son ejemplos de aplicaciones de red.

Aplicación cliente/servidor: Aplicación que se almacena en una posición central en un servidor y a la que tienen acceso las estaciones de trabajo, lo que hace que sean fáciles de mantener y proteger.

Autenticación: Con respecto a la seguridad, la verificación de la identidad de una persona o proceso.

B

Backbone: Núcleo estructural de la red, que conecta todos los componentes de la red de manera que se pueda producir la comunicación.

Balanceo de la carga: En el enrutamiento, la capacidad de un router para distribuir el tráfico a lo largo de todos sus puertos de red que están a la misma distancia desde la dirección destino. Los buenos algoritmos de balanceo de carga usan velocidad de línea e información de confiabilidad. El balanceo de carga aumenta el uso de segmentos de red, aumentando así el ancho de banda efectivo de la red.

Bug: Error en el hardware o en el software que, si bien no impide la ejecución de un programa, perjudica el rendimiento del mismo al no permitir la realización de determinadas tareas o al complicar su normal funcionamiento. Esta palabra también se utiliza para referirse a un intruso.

C

Carga: Parte de una celda, trama o paquete que contiene información de capa superior (datos).

Codificación: Técnicas eléctricas utilizadas para transmitir señales binarias.

Conexión punto a punto: Uno de dos tipos fundamentales de conexión. En ATM, una conexión punto a punto puede ser una conexión unidireccional o bidireccional entre dos sistemas finales ATM. Comparar con conexión punto a multipunto.

Consola: Equipo terminal de datos a través del cual se introducen los comandos en un host.

Convergencia: Velocidad y capacidad de un grupo de dispositivos de internetwork que ejecutan un protocolo de enrutamiento específico para concordar sobre la topología de una internetwork de redes luego de un cambio en esa topología.

Cookie: Pequeño archivo que se genera en el disco duro del usuario desde una página web. Un archivo de esta clase puede registrar las actividades del usuario en la página visitada. Su uso es controvertido, puesto que implica un registro de datos en la computadora del usuario.

Costo: Valor arbitrario, basado normalmente en el número de saltos, ancho de banda del medio, u otras medidas, que es asignado por un administrador de red y utilizado para comparar diversas rutas a través de un entorno de internetwork de redes. Los valores de costo utilizados por los protocolos de enrutamiento determinan la ruta más favorable hacia un destino en particular: cuanto menor el costo, mejor es la ruta

D

Datagrama : Agrupamiento lógico de información enviada como unidad de capa de red a través de un medio de transmisión sin establecer previamente un circuito virtual. Los datagramas IP son las unidades de información primaria de la Internet. Los términos celda, trama, mensaje, paquete y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos

Determinación de ruta: Decisión de cuál es la ruta que debe recorrer el tráfico en la nube de red. La determinación de ruta se produce en la capa de red del modelo de referencia OSI.

Dirección de red: Dirección de capa de red que se refiere a un dispositivo de red lógico, en lugar de físico. También denominada dirección de protocolo

Dirección IP: Dirección de 32 bits asignada a los hosts mediante TCP/IP. Una dirección IP corresponde a una de cinco clases (A, B, C, D o E) y se escribe en forma de 4 octetos separados por puntos (formato decimal con punto). Cada dirección consta de un número de red, un número opcional de subred, y un número de host. Los números de red y de subred se utilizan conjuntamente para el enrutamiento,

mientras que el número de host se utiliza para el direccionamiento a un host individual dentro de la red o de la subred. Se utiliza una máscara de subred para extraer la información de la red y de la subred de la dirección IP.

E

Encabezado: Información de control colocada antes de los datos al encapsularlos para la transmisión en red.

Encapsulamiento: Colocación en los datos de un encabezado de protocolo en particular. Por ejemplo, a los datos de capa superior se les coloca un encabezado específico de Ethernet antes de iniciar el tránsito de red. Además, al conmutar redes que no son similares, toda la trama de una red se puede ubicar simplemente en el encabezado usado por el protocolo de capa de enlace de datos de la otra red. Ver también tunneling.

Enlace punto a punto: Enlace que proporciona una sola ruta preestablecida de comunicaciones de WAN desde las instalaciones del cliente a través de una red de carrier, como, por ejemplo, la de una compañía telefónica, a una red remota. También denominado enlace dedicado o línea arrendada.

Enrutamiento: Proceso de descubrimiento de una ruta hacia el host destino. El enrutamiento es sumamente complejo en grandes redes debido a la gran cantidad de destinos intermedios potenciales que debe atravesar un paquete antes de llegar al host destino.

Enrutamiento del camino más corto: Enrutamiento que reduce al mínimo la distancia o costo de la ruta a través de una aplicación de un algoritmo.

F

Filtro: En general, se refiere a un proceso o dispositivo que rastrea el tráfico de red en busca de determinadas características, por ejemplo, una dirección origen,

dirección destino o protocolo y determina si debe enviar o descartar ese tráfico basándose en los criterios establecidos.

Firewall: Router o servidor de acceso, o varios routers o servidores de acceso, designados para funcionar como búfer entre redes de conexión pública y una red privada. Un router de firewall utiliza listas de acceso y otros métodos para garantizar la seguridad de la red privada.

Flooding: Técnica de transmisión de tráfico utilizada por switches y puentes, en la cual el tráfico recibido por una interfaz se envía a todas las interfaces de ese dispositivo, salvo a la interfaz desde la cual se recibió originalmente la información.

G

Gateway: En la comunidad IP, término antiguo que se refiere a un dispositivo de enrutamiento. Actualmente, el término router se utiliza para describir nodos que desempeñan esta función, y gateway se refiere a un dispositivo especial que realiza conversión de capa de aplicación de la información de una pila de protocolo a otro. Comparar con router.

H

Header (cabecera): Parte inicial de un paquete de datos a transmitir, que contiene la información sobre los puntos de origen y de destino de un envío y sobre el control de errores. Esta expresión se aplica con frecuencia, y de manera errónea, sólo a envío de correo electrónico, por lo que recibe el nombre de “mailheader”, pero normalmente cualquier paquete de datos que se transmite de computadora a computadora contiene una “header”.

Host: Computador en una red. Similar a nodo, salvo que el host normalmente implica un computador, mientras que nodo generalmente se aplica a cualquier sistema de red, incluyendo servidores y routers. Ver también nodo.

IGRP (Protocolo de enrutamiento de gateway interior): Protocolo desarrollado por Cisco para tratar los problemas asociados con el enrutamiento en redes heterogéneas de gran envergadura

IGRP extendido (Protocolo de enrutamiento de gateway interior extendido): Versión avanzada de IGRP desarrollada por Cisco. Ofrece propiedades de convergencia y eficacia operativa superiores, y combina las ventajas de los protocolos del estado de enlace con las de los protocolos por vector distancia. Comparar con IGRP. Ver también OSPF y RIP.

I

Internet: La internetwork de redes más grande del mundo, que conecta decenas de miles de redes de todo el mundo y con una cultura que se concentra en la investigación y estandarización basada en el uso real. Muchas tecnologías de avanzada provienen de la comunidad de la Internet. La Internet evolucionó en parte de ARPANET. En un determinado momento se la llamó Internet DARPA, y no debe confundirse con el término general internet.

internetwork de redes: Agrupamiento de redes interconectadas por routers y otros dispositivos que funciona (de modo general) como una sola red.

L

Latencia : Retardo entre el momento en que un dispositivo solicita acceso a una red y el momento en que se le concede el permiso para transmitir. Intervalo de tiempo que toma el procesamiento de una tarea.

LSA (publicación del estado de enlace): Paquete de broadcast utilizado por los protocolos del estado de enlace que contiene información acerca de vecinos y costos de ruta. Los LSA son utilizados por los routers receptores para mantener sus tablas de enrutamiento. A veces se denomina paquete de estado de enlace (LSP).

M

Mapa de ruta: Método para controlar la redistribución de rutas entre dominios de enrutamiento.

Mensaje: Agrupación lógica de información de la capa de aplicación, a menudo compuesta por una cantidad de agrupaciones lógicas de las capas inferiores, por ejemplo, paquetes. Los términos datagrama, trama, paquete y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

Métrica de enrutamiento: Método mediante el cual un protocolo de enrutamiento determina que una ruta es mejor que otra. Esta información se almacena en tablas de enrutamiento. Las métricas incluyen ancho de banda, costo de la comunicación, retardo, número de saltos, carga, MTU, costo de ruta, y confiabilidad. A menudo denominada simplemente métrica.

MPLS, Multiprotocol Label Switching (Switching de etiquetas multiprotocolo): MPLS es un estándar de la industria sobre el cual se basa la conmutación (switching) de etiquetas, las cuales identifican los diferentes tipos de información sobre la red. La tecnología MPLS le permite a un proveedor de servicio montar sobre su red servicios diferenciados a los cuales se tiene acceso a través del protocolo IP. MPLS permite que los usuarios tengan acceso a la red y se "matriculen" a algunos servicios específicos, sin que esto implique tener acceso a toda la red, es decir que se garantiza la privacidad y seguridad de la Información mediante la creación de redes virtuales privadas, VPNs.

Multicast: Paquetes únicos copiados por una red y enviados a un conjunto de direcciones de red. Estas direcciones están especificadas en el campo de dirección del destino. Comparar con broadcast y unicast.

N

Networking: Interconexión de estaciones de trabajo, dispositivos periféricos (por ejemplo, impresoras, unidades de disco duro, escáneres y CD-ROM) y otros dispositivos.

Nodo: Punto final de la conexión de red o una unión que es común para dos o más líneas de una red. Los nodos pueden ser procesadores, controladores o estaciones de trabajo. Los nodos, que varían en cuanto al enrutamiento y a otras aptitudes funcionales; pueden estar interconectados mediante enlaces y sirven como puntos de control en la red. La palabra nodo a veces se utiliza de forma genérica para hacer referencia a cualquier entidad que tenga acceso a una red y frecuentemente se utiliza de modo indistinto con la palabra dispositivo.

Número de saltos: Métrica de enrutamiento utilizada para medir la distancia entre un origen y un destino. RIP utiliza el número de saltos como su métrica exclusiva.

Número de socket: Número de 8 bits que identifica a un socket. Se pueden asignar como máximo 254 números de socket en un nodo AppleTalk.

O

OSPF (Primero la ruta libre más corta): Protocolo de enrutamiento por estado de enlace jerárquico, que se ha propuesto como sucesor de RIP en la comunidad de Internet. Entre las características de OSPF se incluyen el enrutamiento de menor costo, el enrutamiento de múltiples rutas, y el balanceo de carga.

P

PAP (Protocolo de Autenticación de Contraseña): Protocolo de autenticación que permite que los PPP iguales se autentiquen entre sí. El router remoto que intenta conectarse al router local debe enviar una petición de autenticación A diferencia de CHAP, PAP pasa la contraseña y el nombre de host o nombre de usuario sin cifrar. PAP no evita el acceso no autorizado, sino que identifica el extremo remoto, el router

o el servidor de acceso y determina si a ese usuario se le permite el acceso. PAP es compatible sólo con las líneas PPP. Comparar con CHAP.

Paquete: Agrupación lógica de información que incluye un encabezado que contiene la información de control y (generalmente) los datos del usuario. Los paquetes se usan a menudo para referirse a las unidades de datos de capa de red. Los términos datagrama, trama, mensaje y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

Paquete hello: Paquete multicast utilizado por routers que utilizan ciertos protocolos de enrutamiento para el descubrimiento y recuperación de vecinos. Los paquetes hello también indican que un cliente se encuentra aún operando y que la red está lista.

Protocolo: Descripción formal de un conjunto de normas y convenciones que establecen la forma en que los dispositivos de una red intercambian información.

Protocolo de enrutamiento: Protocolo que logra el enrutamiento mediante la implementación de un protocolo de enrutamiento específico. Entre los ejemplos de protocolo de enrutamiento se incluyen IGRP, OSPF y RIP. Comparar con protocolo enrutado.

Protocolo de enrutamiento por estado de enlace: Protocolo de enrutamiento en el cual cada router realiza un broadcast o multicast de información referente al costo de alcanzar cada uno de sus vecinos a todos los nodos de la internetwork de redes. Los protocolos de estado de enlace crean una vista coherente de la red y por lo tanto no son propensos a bucles de enrutamiento, pero por otro lado para lograr esto deben sufrir dificultades informáticas relativamente mayores y un tráfico más diseminado (comparado con los protocolos de enrutamiento por vector distancia). Comparar con protocolo de enrutamiento híbrido balanceado y protocolo de enrutamiento por vector de distancia

Protocolo de enrutamiento por vector distancia: Protocolo que itera en el número de saltos en una ruta para encontrar el árbol de extensión de ruta más corta. Los protocolos de enrutamiento por vector distancia piden a cada router que envíe su tabla de enrutamiento completa en cada actualización, pero solamente a sus vecinos. Los algoritmos de enrutamiento por vector distancia pueden ser propensos a los bucles de enrutamiento, pero desde el punto de vista informático son más simples que los algoritmos de enrutamiento de estado de enlace. También denominado algoritmo de enrutamiento Bellman-Ford. Comparar con el protocolo de enrutamiento híbrido balanceado y el protocolo de enrutamiento del estado de enlace.

Protocolo enrutado: Protocolo que puede ser enrutado por el router. Un router debe ser capaz de interpretar la internetwork de redes lógica según lo que especifique dicho protocolo enrutado. AppleTalk, DECnet e IP son ejemplos de protocolos enrutados. Comparar con protocolo de enrutamiento.

Proxy: Entidad que, para aumentar la eficiencia, esencialmente reemplaza a otra entidad.

Puerto: Interfaz en un dispositivo de internetwork (por ejemplo, un router). 2. Enchufe hembra en un panel de conmutación que acepta un enchufe macho del mismo tamaño, como un jack RJ-45. En estos puertos se usan los cables de conmutación para interconectar computadores conectados al panel de conmutación. Esta interconexión permite que la LAN funcione. 3. En la terminología IP, un proceso de capa superior que recibe información de las capas inferiores. Los puertos tienen un número, y muchos de ellos están asociados a un proceso específico. Por ejemplo, SMTP está asociado con el puerto 25. Un número de puerto de este tipo se denomina dirección conocida. 4. Volver a escribir el software o el microcódigo para que se ejecute en una plataforma de hardware o en un entorno de software distintos de aquellos para los que fueron diseñados originalmente.

R

Red: Agrupación de computadores, impresoras, routers, switches y otros dispositivos que se pueden comunicar entre sí a través de algún medio de transmisión.

Red corporativa: es la red de una asociación comercial, agencia, escuela u otra organización que une sus datos, comunicaciones, informática y servidores de archivo.

Red interna: Red interna a la que tienen acceso los usuarios con acceso a la LAN interna de una organización.

Redundancia: En internetwork, duplicación de dispositivos, servicios o conexiones, de modo que, en caso de que se produzca una falla, los dispositivos, servicios o conexiones redundantes puedan realizar el trabajo de aquellos en los que se produce la falla. 2. En telefonía, la porción de la información total contenida en un mensaje que se puede eliminar sin sufrir pérdidas de información o significado esencial.

Resumen de ruta: La consolidación de números de red publicados en OSPF e IS-IS. En OSPF, esto hace que un resumen de ruta único se publique a otras áreas a través de un router fronterizo.

RFC (petición de comentarios): Serie de documentos empleada como medio de comunicación primario para transmitir información acerca de la Internet. Algunas RFC son designadas por el IAB como estándares de Internet. La mayoría de las RFC documentan especificaciones de protocolos tales como Telnet y FTP, pero algunas son humorísticas o históricas. Las RFC pueden encontrarse en línea en distintas fuentes.

RIP (Protocolo de información de enrutamiento): Protocolo suministrado con los sistemas BSD de UNIX. El Protocolo de Gateway Interior (IGP) más común de la Internet. RIP utiliza el número de saltos como métrica de enrutamiento.

Ruta por defecto: Una entrada de la tabla de enrutamiento que se utiliza para dirigir las tramas para las cuales el próximo salto no está explícitamente mencionado en la tabla de enrutamiento.

S

Salto: Pasaje de un paquete de datos entre dos nodos de red (por ejemplo, entre dos routers).

Servidor: Nodo o programa de software que suministra servicios a los clientes. Ver también cliente.

Socket: Estructura de software que funciona como un punto final de las comunicaciones dentro de un dispositivo de red (similar a un puerto). 2. Entidad direccionable dentro de un nodo conectado a una red AppleTalk; los sockets son propiedad de procesos de software denominados clientes de socket. Los sockets AppleTalk se dividen en dos grupos: las SAS, que están reservadas para clientes como, por ejemplo, los protocolos principales AppleTalk, y las DAS, que son asignadas de forma dinámica por DDP a pedido de los clientes del nodo. Un socket AppleTalk es conceptualmente similar a un puerto TCP/IP.

Software Cisco IOS (Sistema Operativo de Internetwork): Software de sistema de Cisco que proporciona funcionalidad, escalabilidad y seguridad comunes a todos los productos bajo la arquitectura CiscoFusion. El software Cisco IOS permite la instalación y administración centralizada, integrada y automatizada de internetwork, garantizando al mismo tiempo la compatibilidad con una amplia variedad de protocolos, medios, servicios y plataformas.

Spoofing: Esquema que usan los routers para hacer que un host trate a una interfaz como si estuviera funcionando y soportando una sesión. El router hace spoofing de respuestas a mensajes de actividad del host para convencer a ese host de que la sesión continúa. El spoofing resulta útil en entornos de enrutamiento como DDR, en el cual un enlace de conmutación de circuito se desconecta cuando no existe tráfico

que se deba enviar a través del enlace, a fin de ahorrar gastos por llamadas pagas. 2. La acción de un paquete que ilegalmente dice provenir de una dirección desde la cual en realidad no se lo ha enviado. El spoofing está diseñado para contrarrestar los mecanismos de seguridad de la red, tales como los filtros y las listas de acceso.

T

Tabla de enrutamiento: Tabla almacenada en un router o en algún otro dispositivo de internetwork que realiza un seguimiento de las rutas hacia destinos de red específicos y, en algunos casos, las métricas asociadas con esas rutas.

TACACS (Sistema de Control de Acceso al Controlador de Acceso a la Terminal): Protocolo de autenticación, desarrollado por la comunidad DDN, que suministra autenticación de acceso remoto y servicios relacionados, como, por ejemplo, el registro de eventos. Las contraseñas de usuario se administran en una base de datos central en lugar de administrarse en routers individuales, suministrando una solución de seguridad de red fácilmente escalable.

Tunneling: Arquitectura diseñada para suministrar los servicios necesarios para implementar cualquier esquema de encapsulamiento punto a punto estándar

U

UDP (Protocolo de Datagrama de Usuario): Protocolo no orientado a conexión de la capa de transporte de la pila de protocolo TCP/IP. UDP es un protocolo simple que intercambia datagramas sin confirmación o garantía de entrega y que requiere que el procesamiento de errores y las retransmisiones sean manejados por otros protocolos. UDP se define en la RFC 768

V

VPN (Red Privada Virtual): Una Red Privada Virtual, o Virtual Private Network, VPN, permite establecer una conexión segura a través de una red pública, o Internet. Una VPN permite que el tráfico IP viaje seguro a través de una red pública TCP/IP al

encriptar el tráfico desde una red hasta la otra. Una VPN usa tunneling para encriptar toda la información en el nivel IP.

W

WAN (Red de área amplia): Red de comunicación de datos que sirve a usuarios dentro de un área geográfica extensa y a menudo usa dispositivos de transmisión suministrados por carriers comunes. Frame Relay, SMDS y X.25 son ejemplos de WAN. Comparar con LAN y MAN.

ANEXO 1

https://newlabs.icsalabs.com/icsa/product.php?tid=fghhf456fgh

En este sitio se encuentran todos los proveedores certificados.

http://www.hoise.com/vmw/04/articles/vmw/LV-VM-09-04-18.html

Juniper Networks y Sana Security Inc. utilizan defensa en profundidad como una solución de seguridad altamente efectiva.

En este articulo se demuestra como la estrategia de seguridad "defensa en profundidad" proporciona una solución de seguridad simple y comprensiva que puede ser aplicada a infraestructuras de tecnologías heterogéneas.

http://www.google.com.sv/url?sa=t&ct=res&cd=2&url=http%3A//service.escapenet.ch/publisher/pictures/102/Zugriffssysteme_-_WatchGuard_Erika_Jacobs.pdf&ei=xqYGQ5aAIK64aoWa7KkO

Utiliza la estrategia de seguridad "defensa en profundidad" como su solución principal para proveer seguridad de redes.

En la página #4 se muestra como todos los productos de WatchGuard ofrecen una solución de seguridad multicapa aplicando la estrategia de seguridad "defensa en profundidad".

http://mx.sun.com/backissues/2005-0218/

SUN utiliza defensa en profundidad como solución por medio de capas en lugar de utilizar seguridad puntual. En el apartado referente a *defensa en profundidad* se da a conocer como esta estrategia de seguridad es altamente efectiva al momento de la implementación de soluciones de seguridad de redes.

http://securityresponse.symantec.com/avcenter/security/Content/security.articles/defense.in.depth.html

Symantec utiliza defensa en profundidad como una solución. En el apartado #1 de este artículo, se explica como la aproximación mediante la defensa en profundidad proporciona una protección efectiva contra los nuevos tipos de amenazas de seguridad que vas surgiendo.

http://enterprisesecurity.symantec.com/industry/power/article.cfm?articleid=3186
Defensa en profundidad es recomendada por Bill campbell CISSP vicepresidente de las soluciones verticales y estratégicas de Symantec Corporation. En la sección de defensa en profundidad de este artículo se menciona como esta estrategia de seguridad va mas allá del simple hecho de asegurar el perímetro de red. Así también, como la defensa en profundidad combina productos y servicios para lograr de manera efectiva la continuidad de la empresa, el apego a estándares de seguridad de la cyber industria y evitar costosas interrupciones asociadas con las brechas de seguridad de información.

http://www.cisco.com/en/US/products/hw/switches/ps708/products_customer_success_story0900aecd8022d5f0.html
Cisco Systems utiliza defensa en profundidad.
En el apartado de la solución ofrecida por CISCO, describe como la aproximación de la estrategia de seguridad " defensa en profundidad" es aplicada para el diseño de la seguridad de la red.

http://www.sans.org/sansfire2004/faculty.php
Consultores de sans y autores de libros reconocidos como por ejemplo Mastering Cisco Routers enseñan defensa en profundidad.
En la seccion de Chris Brenton se da a conocer como todos los dispositivos de internetworking y protocolos aportan un respaldo valioso para poder conseguir la implementación de la estrategia de seguridad "defensa en profundidad",

http://www.sans.org/rr/papers/9/710.pdfSans recomienda defensa en profundidad. En el primer apartado del capitulo se explica el porque de esta solución en particular y como mediante la aplicación de esta estrategia de seguridad se protege a la red corporativa de manera segura y eficaz.

http://www.iss.net/issEn/delivery/prdetail.jsp?type=ISS&oid=21051
Internet Security Systems patenta la nueva tecnología que utiliza defensa en profundidad para evitar los ataques por medio de código que ponga en riesgo la

seguridad de los datos de la corporación, el articulo describe el porque de la adquisición de la tecnología de inspección de comportamiento preventivo y como este provee defensa en profundidad al evitar el compromiso de la seguridad del equipo de computo de la corporación.

http://www.firewall-reviews.com/

Equipo de proveedores en donde se puede implementar defensa en profundidad. Estos proveedores y equipos están certificados por icsalab.

http://www.checkpoint.com/products/industries/government/government_tips.html#tip2

Checkpoint provee información de seguridad al gobierno e incluye defensa en profundidad. En la sección referente a defensa en profundidad de este articulo se explica que no es suficiente la seguridad que provee un solo firewall contra los ataques y que se necesita seccionar la seguridad a fin de proporcionar una mayor cobertura en la seguridad.

http://www.cert.org/incident_notes/IN-2003-01.html

cert recomienda defensa en profundidad como una solución para protegerse de código malicioso. En la sección de las soluciones de este articulo se explica el porque es importante poseer varios niveles de seguridad o controles de acceso en lugar de poseer un solo nivel de protección, aplicando de esta forma la estrategia de seguridad “defensa en profundidad”

http://www.arubanetworks.com/technology/whitepapers/defenseindepth/

aruba network recomienda seis estrategias para la defensa en profundidad. Estas estrategias tienen como objetivo el asegurar de manera efectiva y segura el control de acceso, la integridad de los datos y la privacidad de los mismos.

http://www.cyberguard.com/news_room/white_papers/CG_Defense_in_Depth.html?lang=de_EN

Cyberguard aplica una estrategia de defensa en profundidad para fortalecer sus tecnologías de firewalls. Se explica en este documento como aplicar defensa en profundidad mediante los diferentes productos que la compañía posee.

http://www.nsa.gov/about/about00019.cfm#6

Concepto de estrategia de seguridad defensa en profundidad. En el punto #6 se responde de a la pregunta de que defensa en profundidad y como ayuda a la seguridad dentro de la red.

www.nsa.gov/snac/support/defenseindepth.pdf

nsa ve la estrategia defensa en profundidad de una manera practica para asegurar la información que viaja a través de la red. Este docume32nto detalla como mediante la implementación de la estrategia de seguridad "defensa en profundidad" se puede lograr una mejor protección de la red.

www.nsa.gov/snac/support/WORMPAPER.pdf

La nsa recomienda defensa en profundidad par solucionar los problemas de virus.

El documento explica como se puede proteger mejor la red corporativa de la amenaza que representan los virus mediante la implementación de defensa en profundidad.

http://www.networkworld.com/columnists/2004/081604johnson.html

Recomienda la implementación de la estrategia defensa en profundidad.

En este articulo se da a conocer la importancia de la implementación en la actualidad de la estrategia de seguridad "defensa en profundidad" y como ayuda en la protección de la red corporativa.

http://www.avolio.com/columns/defense-in-depth.html

Información acerca de defensa en profundidad, la información proporcionada por este articulo ayuda a comprender el porque es importante la implementación de la estrategia de seguridad "defensa en profundidad" para lograr la protección de la red corporativa

http://www.axial.co.uk/mcafee/entercept_products.asp

McAfee utiliza defensa en profundidad como soluciones para las organizaciones, en el articulo se detalla la aproximación que utiliza mediante la implementación de la seguridad en profundidad y como esta ayuda en la seguridad de la red corporativa para la prevención de las infecciones por virus.

http://emea.windowsitpro.com/EMEA/Article/ArticleID/47195/EMEA_47195.html

Porque es tan importante la defensa en profundidad. El articulo describe la importancia de la implementación de la estrategia de seguridad "defensa en profundidad", opiniones y comentarios sobre esta estrategia de seguridad

http://64.233.187.104/search?q=cache:MgAbl6xyNY8J:proceedings.ndia.org/3690/Wednesday_Breakout_RoomA/3COMDesktop.ppt+3com+why+use+defense+in+depth&hl=es

3com y defensa en profundidad. El documento proporciona información sobre el costo y riesgos que se corren sin la implementación de la estrategia de defensa en profundidad y los beneficios que se obtienen cuando esta es implementada.

http://www.borderware.com/press/releases.php?action=v&id=144

Artículo que detalla la unión de Borderware y 3com con el objeto de implementar defensa en profundidad en las soluciones para protección de redes.

http://www.gcn.com/22_29/news/23680-1.html

Noticia acerca del FBI que utiliza reglas debajo de defensa en profundidad. Este articulo destaca como mediante la utilización de la estrategia de seguridad "defensa en profundidad" se toman todas las medidas de seguridad necesarias para no dejar ninguna brecha por donde la información o los usuarios puedan se objeto de cualquier ataque.

ANEXO 2

Los videos de configuraciones pueden ser consultados desde la pagina web menu_videos.htm ubicado en la carpeta anexo2 en el cd anexo a esta tesis:

- Video **“Protocolo RIP en el Router Cliente”**
- Video **“Configuración VPN en el Router Cliente”**
- Video **“Probando la VPN”**
- Video **“Configuración de Interfaces Pix FIrewall”**
- Video **“Configuración de AAA en el Pix FIrewall”**
- Video **“Probando control de acceso en el Pix Firewall”**