UNIVERSIDAD DON BOSCO
Faculta de Ingeniería

Trabajo de Graduación para optar al grado de
Ingeniero en Ciencias de la Computación

ESTUDIO DE LA SITUACIÓN ACTUAL EN MATERIA DE SEGURIDAD EN REDES E IMPLEMENTACIÓN DE UN PROTOTIPO BASADO EN FIREWALL UTILIZANDO IOS CISCO

PRESENTADO POR:

Jorge Alberto Barrera
Karla Patricia Merino Portillo
Darwing Alberto Martinez Navarrete

Noviembre de 2005

El Salvador, Centro América

INDICE DE CONTENIDOS

.....vi
INTRODUCCIÓN.....1
CAPÍTULO 1. GENERALIDADES DEL PROYECTO.....3
1.1 OBJETIVOS.....3
1.1.1 OBJETIVO GENERAL.....3
1.1.2 OBJETIVOS ESPECÍFICOS.....3
1.2 ALCANCES.....4
1.3 LIMITACIONES.....5
1.4 DELIMITACIÓN.....7
CAPÍTULO 2. SITUACIÓN ACTUAL.....8
.....8
DEFINICIÓN DE POLÍTICAS DE SEGURIDAD.....8
2.1.1 POLÍTICAS DE SEGURIDAD.....8
2.1.2 PASOS PARA LA CREACIÓN DE LAS POLÍTICAS DE SEGURIDAD EN UNA ORGANIZACIÓN [14] 9
2.1.3 ELEMENTOS DE UNA POLÍTICA DE SEGURIDAD INFORMÁTICA [13].....11
2.1.4 POLÍTICAS DE SEGURIDAD EN LA ACTUALIDAD.....13
2.1.5 VALORACIONES EN LA IMPLEMENTACIÓN DE UNA PSI.....14
2.2 IDENTIFICACIÓN DE AMENAZA.....15
2.2.1 AMENAZAS DE PERSONAS (INTERNOS – EXTERNOS).....16
2.3 POLITICAS ORGANIZACIONALES.....17
2.3.1 A NIVEL FÍSICO.....18
2.3.2 ANTE DESASTRES NATURALES.....19
2.3.3 PARA LOS USUARIOS.....19
2.3.4 USO DE CLAVES DE ACCESO.....20
2.4 POLÍTICAS TÉCNICAS.....21
2.5 ESTRATEGIA DE SEGURIDAD.....24
.....24
2.6 RECOMENDACIONES EN EL MANEJO DE LA ADMINISTRACIÓN DE ACCESOS.....24
CAPÍTULO 3. DESARROLLO DE ESTUDIO DE MERCADO.....26
3.1 INTRODUCCIÓN.....26
3.2 PUNTOS A CONSIDERAR PARA REALIZAR LA ENCUESTA.....27
3.3 DISEÑO DE LA INVESTIGACIÓN.....28
3.3.1 OBJETIVO GENERAL.....28
3.3.2 OBJETIVOS ESPECÍFICOS.....28
3.4 METODOLOGÍA.....29
3.4.1 UNIDAD DE INVESTIGACIÓN.....29
3.4.2 DESCRIPCIÓN DE LA DEMANDA.....30
3.4.3 COBERTURA.....33
3.5 JUSTIFICACIÓN DEL USO DE UN ROUTER CÓMO FIREWALL.....34
3.6 OPCIONES EN EL MERCADO DE IOS FIREWALL DE CISCO.....35
3.7 GRÁFICOS Y RESULTADOS OBTENIDOS EN LA ENCUESTA.....43
3.8 CONCLUSIONES DEL ESTUDIO DE MERCADO.....55
3.9 CASO PRÁCTICO. PROBLEMA A RESOLVER.....58
CAPÍTULO 4. IMPLEMENTACIÓN DEL FIREWALL.....60
4.1 TIPOS DE ATAQUES [8].....60

4.1.1 FUENTES DE ORIGEN DE LOS ATAQUES DOS / DDOS....60
4.1.2 DETECCIÓN DE ATAQUES DoS....61
4.1.2.1 ATAQUES COMUNES....61
4.1.2.2 DEFENSAS CONTRA DOS/DDOS....70
4.1.3 ATAQUES DE AUTENTICACIÓN....71
4.1.4 ROUTING PROTOCOLS [3]....75
4.2 IMPLEMENTACIÓN DE TÉCNICAS DE FILTRADO....77
4.2.1 LISTAS DE CONTROL DE ACCESO (ACL) [4]....77
4.2.1.1 COMPRENDER EL FILTRADO DE PAQUETE....77
4.2.2 FILTRADO DE URL[3]....79
4.2.2.1.1 VENTAJAS DE USAR FILTRADO DE URL....80
4.2.2.1.2 RESTRICCIONES DE FILTRADO DE URLS....81
4.3 CONTROL DE ACCESO BASADO EN CONTEXTO (CBAC) [3]....82
4.3.1 FUNCIONES DE CBAC....82
4.3.2 PROTOCOLOS SOPORTADOS POR CBAC....84
4.3.3 FUNCIONAMIENTO DE CBAC....84
4.3.4 LIMITACIONES DE CBAC....85
4.3.5 CONFIGURACIÓN DE CBAC....86
4.3.6 USO DE CBAC PARA PREVENCIÓN Y DETECCIÓN DE ATAQUES DOS ..86
4.4.1 COMPONENTES DE QOS....88
4.4.2 NBAR Y SU CLASIFICACIÓN....88
4.4.3 NBAR Y FILTRADO DE TRÁFICO....89
4.4.4 RESTRICCIONES DE NBAR....90
4.4.5 CONFIGURACIÓN BÁSICA DE NBAR....90
4.5 SISTEMAS DE DETECCIÓN DE INTRUSOS (IDS) [3]....91
4.5.1 ¿QUÉ ES UN SISTEMA DE DETECCIÓN DE INTRUSOS?....91
4.5.2 IMPLEMENTACIÓN DE IDS....92
4.5.3 CONFIGURACIÓN DE IDS....94
4.6 NAT [7]....99
4.7 TÉCNICAS DE ENCRIPTADO....100
4.7.1 REDES VIRTUALES PRIVADAS (VPN) [7]....100
4.7.2.1 VENTAJAS DE IPSEC....102
4.7.2.2 BENEFICIOS QUE APORTA IPSEC....103
4.7.2.3 IPSEC SE DISTINGUEN POR LOS SIGUIENTES COMPONENTES....104
4.7.2.3.1 EL PROTOCOLO AH....104
4.7.2.3.2 FUNCIONAMIENTO AH....106
4.7.2.3.3 EL PROTOCOLO ESP....106
14.3.4 FUNCIONAMIENTO ESP....108
4.7.2.3.4 FUNCIONAMIENTO ESP....109
4.7.2.3.5 LOS MODOS DE TRANSPORTE Y DE TUNEL....109
4.7.2.3.6 IKE EL PROTOCOLO DE CONTROL....111
4.7.2.4 APLICACIONES PRÁCTICAS DE IPSEC....113
4.7.3 REQUERIMIENTOS BÁSICOS DE UNA VPN....120
4.7.4 VENTAJAS DE UNA VPN....121

4.7.5 TIPOS DE VPN....121
4.8 TÉCNICAS DE AUTENTICACIÓN....123
4.8.1 AUTENTICACIÓN PROXY (AP) [3]....123
4.8.2 CARACTERÍSTICAS DEL AP....123
4.8.3 USO DE AUTHENTICATION PROXY....125
4.8.4 CUANDO USAR AP....125
4.8.5 DONDE USAR AP....126
4.8.6 LIMITACIONES DE AP....127
4.8.7 CONFIGURACIÓN AP....128
4.8.8 AAA (AUTENTICACIÓN, AUTORIZACION, CONTEO)....128
4.8.8.1 AUTENTICACIÓN....129
4.8.8.2 AUTORIZACIÓN....129
4.8.8.3 CONTEO....129
4.8.8.4 BENEFICIOS DE AAA....129
4.8.8.5 TACACS....130
4.8.8.5.1 AUTENTICACIÓN....131
4.8.8.6 RADIUS (REMOTE AUTHENTICATION DIAL-IN USER SERVICE)....132
4.8.8.6.1 FORMA DE APLICACIÓN....132
4.8.8.7 COMPARACIÓN ENTRE TACACS+ Y RADIUS....134
4.9 TCP / INTERCEPT TCP SYNFLOOD PREVENTING [3]....135
4.9.1 TCP SYN FLOOD ATTACKS O ATAQUES DE INUNDACIÓN....135
4.9.2 MODOS TCP INTERCEPT....136
4.9.2.1 MODO DE INTERCEPCIÓN....136
4.9.2.2 MODO WATCH (MODO RELOJ)....137
4.10 RATE LIMITING (LIMITACIÓN - RANGO DE TARIFA) [3]....140
4.10.1 ICMP RATE LIMITING....141
4.11 REVERSE PATH FORWARDING (REENVIO DE TRAYECTORIA REVERSA) [3] 141
4.11.1 USO DE RPF....142
4.11.2 LIMITACIONES DE RPF....142
4.11.3 CONFIGURACIÓN DE RPF....143
4.12 TÉCNICAS DE FAILOVER [3]....144
4.12.1 TRASLADO DE DIRECCIONES Y REDUNDANCIA....144
4.12.1.1 REDUNDANCIA CON TRASLADO DE DIRECCIONES ESTÁTICAS HACIENDO USO DE HSRP....144
4.12.1.2 PROCESO DE LA REDUNDANCIA CON HSRP....145
4.12.2 CARACTERÍSTICAS Y RESTRICCIONES DE SNAT FAILOVER....148
4.12.3 SNAT CON HSRP....149
4.12.3.1 CONFIGURACIÓN DE HSRP CON SNAT FAILOVER....150
4.12.4 CONFIGURAR EL TRASLADO DE DIRECCIONES....150
4.13 PLANTEAMIENTO DE SOLUCIÓN A IMPLEMENTAR....151

CAPÍTULO 5. DISEÑO DEL SOFTWARE....155
5.1 INTRODUCCIÓN....155
5.2 PLANTEAMIENTO DEL PROBLEMA....155
5.3 PLANIFICACIÓN DEL SOFTWARE....155
5.3.1 ÁMBITO DEL SOFTWARE....155
5.3.1.1 SISTEMA CONFIGURACIÓN Y MONITOREO....155
5.3.2 ESTIMACIÓN DE RECURSOS....156
5.3.2.1 RECURSOS HUMANOS....156
5.4 PROCESOS....157
5.4.1 INICIO DE SESIÓN (IS)....157
5.4.2 REGISTRO DE USUARIO (RU)....157
5.4.3 AUTOMATIZACIÓN DE CONFIGURACIONES (AC)....157
5.4.4 INTERFACE DEL USUARIO Y FACILIDADES DE CONTROL (IUFC)....158
5.4.5 ELABORACIÓN DE REPORTES E INFORMES (ERI)....158
5.4.6 GESTIÓN DE LA BASE DE DATOS (GBD)....158
5.4.7 TABLA DE ESTIMACIÓN BASADA EN EL PROCESO....159
5.4.8 ANÁLISIS DEL SISTEMA....160
5.4.8.1 PARTICIÓN DEL PROBLEMA....160
5.5 HERRAMIENTAS UTILIZADAS PARA EL DESARROLLO DEL SOFTWARE...161
5.5.1 SOFTWARE A UTILIZAR....161
5.5.2 INTERCONEXIÓN DE TECNOLOGíAS UTILIZADAS....165
5.5.3 DESCRIPCIÓN DE DIAGRAMAS DE FLUJO....166
5.5.3.1 DIAGRAMA DE CONTEXTO....166
5.5.4 PROCESO DE CONFIGURACIÓN DE POLÍTICAS....167
5.5.5 PROCESO DE CONFIGURACION DEL SISTEMA DE MONITOREO....168
5.6 DISEÑO DE LA INTERFASE....169
5.6.1 REQUISITOS DE HARDWARE Y SOFTWARE....172
5.6.2 ESTRUCTURA DE DIRECTORIOS DEL SISTEMA....173
CONCLUSIONES....174
GLOSARIO....178
A....178
B....178
C....179
D....179
E....180
F....180
G....181
H....181
I....181
L....182
N....182
P....183
R....184
S....184
T....185
U....185

V....186
W....187
X....187
FUENTES DE INFORMACIÓN....188
BIBLIOGRAFÍA....188
ANEXOS....190
ANEXO 1. LISTADO DE PREGUNTAS DE LA ENCUESTA....190
ANEXO 2. ESPECIFICACIONES TÉCNICAS DEL ROUTER [4]....196
....196
ANEXO 3. ESPECIFICACIONES TÉCNICAS DE IOS Cisco [4]....206
ANEXO 4.CONFIGURACIÓN BÁSICA DE UN DISPOSITIVO CISCO [4]....236
ANEXO 5. PROTOCOLO RIP [4]....259
ANEXO 6. MANUAL DE USUARIO....316
ANEXO 7. PROGRESO EN CONFIGURACIÓN DE TÉCNICAS 338

INTRODUCCIÓN

Con el incremento de ataques de hackers, gusanos, virus y otras amenazas, la seguridad se convierte en el mayor problema en la actualidad y más aun sabiendo que ésta es un recurso valioso al igual que todos los activos de una empresa. La seguridad por lo tanto debe ser diseñada, implementada, controlada y administrada.

El escenario actual nos muestra, cómo las organizaciones a escala mundial han entendido que el uso de la tecnología de información y el acceso a Internet representa una progresiva aceleración en los avances operativos con incidencia en la forma de hacer negocios, e incluso, en la forma de trabajar. Adicionalmente, ha representado un medio de comunicación efectivo y oportuno con clientes, proveedores, empresas e instituciones relacionadas, que permite el intercambio de información para fines comerciales sin importar la ubicación de ellos siendo ésta una de las mayores ventajas.

"El NCSA (US National Computer Security Agency) comenta que la mayoría de ataques no son detectados. El 88 % de estos ataques son exitosos y sólo un 5 % son detectados. También el NCSA comenta que el 80 % de los ataques electrónicos investigados por el FBI (US Federal Bureau of Investigation) están relacionados con Internet". **[12]**

"Viéndose afectadas empresas tanto dedicadas a Internet (comercio electrónico, servidores Web) como aquellas que realizan transacciones a través de Internet (universidades y organismos públicos, bancos, etc.). La ignorancia sobre los "hackers" hace que muchas empresas se desentiendan del problema de la seguridad, viéndose muy comprometida su seguridad y con ello sus recursos". **[12]**

Sin embargo, hoy en día existe un riesgo mayor de que los mensajes transmitidos tanto dentro, como fuera de las empresas, puedan ser interceptados por usuarios maliciosos usando herramientas de tipo “sniffing” (método que se utiliza para determinar datos muy confidenciales monitoreando los paquetes de datos al nivel de protocolo de Internet IP) y de re-direccionamiento de tráfico; así mismo, las contraseñas pueden ser capturadas o deducidas y constantemente surgen nuevas vulnerabilidades en el entorno de redes informáticas.

Los hechos mencionados anteriormente, pueden ser aprovechados por personas no autorizadas para beneficios diferentes a los originalmente destinados. Además muchos de los problemas de seguridad que surgen día con día se deben a interconexiones entre redes fiables (red privada) y redes no fiables (Internet), para ello existen sistemas que imponen políticas de seguridad, también conocidos como Firewall o “Muro de Fuego” (***Un Firewall sirve para impedir que un atacante pase de una red a otra***, en el caso típico un Firewall se sitúa entre una red no fiable *(Internet)* y una fiable *(una red interna*)), ofreciendo un control de tráfico entre diferentes áreas de la red; optimizando muchas funciones y ofreciendo soluciones, siendo el propósito primordial el de controlar el acceso a los recursos.

Debido a la problemática existente surge el interés de descubrir alternativas que solventen de manera eficiente los problemas relacionados con la seguridad de una red privada, una de ellas es la implementación de Firewall utilizando enrutadores Cisco para asegurar el perímetro de la red. Buscando con ello que los enrutadores incluyan en su configuración técnicas necesarias para que actúen como un Firewall.

CAPÍTULO 1. GENERALIDADES DEL PROYECTO

1.1 OBJETIVOS

1.1.1 OBJETIVO GENERAL

"Desarrollar un Estudio de la Situación Actual en Materia de Seguridad en Redes de Empresas Salvadoreñas que permita visualizar el estado existente de éstas e Implementación de un Prototipo basado en Firewall utilizando enrutadores con IOS Cisco"

1.1.2 OBJETIVOS ESPECÍFICOS

- Efectuar un estudio de mercado para el análisis de la situación actual en materia de seguridad de redes, a fin de determinar niveles de inversión de las empresas en ésta área y sus expectativas de implementación.

- Realizar un estudio para mostrar las diversas opciónes que tienen las empresas al momento de decidir incorporar un sistema de seguridad en sus redes privadas.

- Diseñar e Implementar un software para la generación de reportes estadísticos de eventos registrados por el Firewall.

- Diseñar e Implementar un software para la configuración de enrutadores con funciones de Firewall.

- Implementar un prototipo de Firewall aplicando las técnicas de protección contra ataques más comunes, instalando una red de tres computadoras y dos enrutadores Cisco modelo 1750 con versión de software IOS 12.2 (27) que soporta la funcionalidad de Firewall, IDS y VPN.

- Documentar el proceso de configuración e implementación del prototipo a presentar.

1.2 ALCANCES

Se pretende realizar los siguientes alcances:

- Definir mediante Estudio de Mercado las ventajas y desventajas, tanto económicas como técnicas de las diversas opciónes que tienen las empresas al momento de decidir incorporar un sistema de seguridad.

- La recolección de información para el estudio de mercado se realizará por medio de encuestas hechas a las empresas.

- Elaborar documentación en formato de video, siendo una guía interactiva que contendrá las diversas configuraciones a realizar en el enrutador con funcionalidad de Firewall.

- El prototipo de Firewall incluirá sistema de Failover, el cual será un respaldo para la protección de la red.

- El Firewall a implementar será capaz de detectar los siguiente ataques:
    - Ataques de rastreo de tráfico.
    - Ataques de Negación de servicio.
    - Ataques de Acceso no autorizado.

- Demostrar el funcionamiento del Firewall mediante la realización de los ataques mencionados en el punto anterior.

1.3 LIMITACIONES

- La implementación del firewall sólo se desarrollará con 2 enrutadores Cisco, específicamente el modelo Router 1750 con versión de software IOS 12.2 (27) que soporta la funcionalidad de Firewall, IDS y VPN.

- El estudio de mercado estará orientado específicamente a la pequeña y mediana empresa.

- Para la realización del estudio de mercado, **se hará en el transcurso del trabajo de graduación** estableciendo según el cronograma el diseño de entrevista, estudio y resultados.

- Se utilizará solamente la cantidad de equipo establecido por lo cuál la demostración de Failover será únicamente en un extremo de la red.

- Para efectos de demostración de la VPN, se hará uso de dos MODEM RAD ASMI 50; esto permitirá simular la conexión a Internet entre las redes.

- Detectar y proteger de ataques DoS, spoofing, routing, utilizando las siguientes técnicas:
  - Rate Limiting.
  - RPF (Reverse Path Forwarding/ Camino Inverso Remitido).
  - Black Hole.
  - ACL´s (Access Control List / Listas de control de Acceso) estándar y extendidas.
  - Filtrado de URL´s.
  - CBAC (Contex Based Access Control / Control de Acceso basado en Contexto).
  - NBAR (Network Based Application Recognition / Aplicación de Red basado en Reconocimiento).

- Proveer una conexión protegida entre dos redes de área local, utilizando VPN (Virtual Private Network / Red Privada Virtual), IDS (Intrusion Detection System / Sistema de Detección de Intrusos), NAT (Network Address Traslation / Traslado de Direcciones de Red), PAT (Port Address Traslation / Traslado de Direcciones de Puerto) y autenticación de usuarios mediante AP (Authentication Proxy / Autenticación por Proxy).

- Utilizar IPSec con soporte del algoritmo de encriptación DES y función de Hashing MD5 para asegurar la integridad de los datos.

El Firewall a implementar no será capaz de proteger a la red privada de ataques de Virus.

1.4 DELIMITACIÓN

Para efectos de investigación en cuanto al desarrollo del Firewall y refiriéndose a la recolección y análisis de datos, se efectuará con las organizaciones o empresas cuyos fines estén encaminados al uso de redes informáticas para la transferencia de información a través de Internet. Dentro de este gran universo de entidades existe un subgrupo el cuál resulta de interés y más factible recopilar información. Ya definidos los parámetros de selección, las entidades consideradas como pequeñas o medianas empresas serían sobre las que se recolectaría la información.

De una manera cuantitativa y haciendo referencia al grupo seleccionado, los requerimientos serían:

- Que las empresas estén ubicadas geográficamente en El Salvador y que su sede se encuentre en la capital.
- Que las empresas tengan como objetivo primordial el proteger la información.
- Que posean enrutadores Cisco o tengan la capacidad de adquirirlos.

También es necesario efectuar la recolección en un nivel cualitativo refiriéndose con esto a los trabajadores o encargados de la administración de las redes. Esto requiere que posean conocimientos amplios en cuanto a la administración y mantenimiento así como también los permisos necesarios para la realización de modificaciones dentro de la red.

Basándose en lo expuesto inicialmente se delimita el área sobre el cuál se desarrollará el proyecto en cuestión.

CAPÍTULO 2. SITUACIÓN ACTUAL

DEFINICIÓN DE POLÍTICAS DE SEGURIDAD

2.1.1 POLÍTICAS DE SEGURIDAD

La propia complejidad de la red es una dificultad para la detección y corrección de los múltiples y variados problemas de seguridad que van apareciendo. Actualmente han ido aumentando las acciones poco respetuosas de la privacidad y de la propiedad de recursos y sistemas; “Hackers”, “crakers”, entre otros, han hecho aparición en el vocabulario ordinario de los usuarios y de los administradores de las redes. Además de las técnicas y herramientas criptográficas, es importante reiterar que un componente muy importante para la protección de los sistemas consiste en la atención y vigilancia continua y sistemática por parte de los responsables de la red.

Proveer acceso a los servicios de la red de una empresa y proveer acceso al mundo exterior a través de la organización, otorga al personal e institución muchos beneficios. Sin embargo, a mayor acceso que se provea, mayor es el peligro de que incremente la vulnerabilidad en la red.

El desarrollo de una política de seguridad comprende la identificación de los activos organizativos, evaluación de amenazas potenciales, la evaluación del riesgo, implementación de las herramientas y tecnologías disponibles para hacer frente a los riesgos y el desarrollo de una política de uso. Debe crearse un procedimiento de auditoría que revise el uso de la red y servidores de forma periódica.

2.1.2 PASOS PARA LA CREACIÓN DE LAS POLÍTICAS DE SEGURIDAD EN UNA ORGANIZACIÓN [14]

- ✓ **Identificación de los activos organizativos:**

  Consiste en la creación de una lista de todos los objetos que precisen protección.

  Por ejemplo: Hardware: Estaciones de trabajo y equipos de telecomunicación.
  Software: Programas fuente, útilidades, programas de diagnóstico, sistemas operativos, programas de comunicaciones.
  Datos: Copias de seguridad, registros de auditoria, bases de datos.

- ✓ **Valoración del riesgo:**

  Conlleva la determinación de lo que se necesita proteger. No es más que el proceso de examinar todos los riesgos, y valorarlos por niveles de seguridad.

- ✓ **Definición de una política de uso aceptable (Creación de políticas):**

  Las herramientas y aplicaciones forman la base técnica de la política de seguridad, pero la política de uso aceptable debe considerar aspectos como los listados a continuación:

  - ¿Quién tiene permiso para usar los recursos?
  - ¿Quién esta autorizado a conceder acceso y a aprobar los usos?
  - ¿Quién tiene privilegios de administración del sistema?
  - ¿Qué hacer con la información confidencial?
  - ¿Cuáles son los derechos y responsabilidades de los usuarios?

  Por ejemplo, al definir los derechos y responsabilidades de los usuarios:

  - Si los usuarios están restringidos y cuáles son sus restricciones.
  - Si los usuarios pueden compartir cuentas o dejar que otros usuarios útilicen sus cuentas.
  - Cómo deberían mantener sus contraseñas los usuarios.
  - Con qué frecuencia deben cambiar sus contraseñas.

- Si se facilitan copias de seguridad o los usuarios deben realizar las suyas.

- ✓ **Entrenamiento de personal en estas políticas:**

  Como parte del plan de creación de políticas de seguridad en una organización esta un punto clave el cuál es, entrenar a los empleados o usuarios de la red quienes estaran sujetos a estas normativas previamente definidas.

  Como parte de este entrenamiento se recomienda que se provea al usuario de material ya sea escrito o digital, en el cual se le desglocen las políticas de seguridad.

  Asi mismo, debe de haber personal capacitado para atender las dudas de los usuarios o para ayudarlos a la hora de enfrentarse ante una situación en la que deben de tomarse en cuenta para ser resuelto las politicas de seguridad ya definidas.

  Asi también, debe capacitarse al personal de informática de manera que; esten capacitados a la hora de enfrentar cualquier situación o anomalía en el funcionamiento de la red.

  Siendo el Administrador de red, quien principalmente debe estar preparado y tener cierto grado de experiencia en circunstancias que tengan que ver con la seguridad de una red informática y con sus recursos y en base a las políticas de seguridad darle respuesta a tales situaciónes.

- ✓ **Implementacion de las políticas:**

  Una vez definidas y valoradas las políticas de seguridad, estas deben llevarse al campo experimental es decir; al acontecer cotidiano en las labores de los usuarios en una organización.

- ✓ **Monitorear las políticas de seguridad:**

  Liderado por el Administrador de red, debe haber un equipo integrado por personal capacitado que le de un seguimiento a las políticas de seguridad en la organización y la manera como éstas se acoplan a las necesidades de los usuarios.

  En caso de ser necesario, se recomienda realizar una retroalimentación en caso de que alguna política de seguridad no este siendo muy útil en las situaciónes de la red informática. Pudiendo ser esta descartada o ajustarla a una nueva normativa que ayude a solventar algún conflicto o situación en la red.

2.1.3 ELEMENTOS DE UNA POLÍTICA DE SEGURIDAD INFORMÁTICA **[13]**

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 útilidad 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 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.

2.1.4 POLÍTICAS DE SEGURIDAD EN LA ACTUALIDAD

Actualmente la seguridad informática ha alcanzado gran auge, dadas las condiciones cambiantes 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.

Dicha situación ha llevado a la aparición de nuevas amenazas en los sistemas computarizados. Consecuentemente, muchas organizaciones gubernamentales y no gubernamentales internacionales han desarrollado documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones con el objeto de obtener el mayor provecho de estas ventajas, y evitar el uso indebido de la mismas.

Esto puede ocasionar serios problemas en los bienes y servicios de las empresas en el mundo.

En este sentido, ***las políticas de seguridad informática (PSI) surgen como una herramienta organizacional para concienciar a cada uno de los miembros de una organización sobre la importancia y la sensibilidad de la información y servicios críticos que favorecen el desarrollo de la organización y su buen funcionamiento.***

Son muchos los casos que en todo el mundo suceden, todos los dias desde los más simples ataques a una red con la finalidad de inestabilizarla hasta los ataques que hacen perder a grandes empresas grandes cantidades de dinero, aparte de que merma el prestigio que estas tienen en el mercado.

2.1.5 VALORACIONES EN LA IMPLEMENTACIÓN DE UNA PSI

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

Se deberá tener en cuenta que la implementación de Políticas de Seguridad, trae ligados 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 operatoria de la organización, tanto técnica como administrativamente.

Por esto, será necesario calcular 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 al resto de la organización con el fin de otorgar visibilidad a los actos de la administración.

Una PSI informática deberá abarcar

1

- 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. [15]

- 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 pasará o cuándo algo sucederá; ya que no es una sentencia obligatoria de la ley.

- 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.

2.2 IDENTIFICACIÓN DE AMENAZA

Se suele dividir las amenazas existentes según su ámbito de acción:

- Desastre del entorno (Seguridad Física).

- Amenazas del sistema (Seguridad Lógica).

- Amenazas en la red (Comunicaciones).

2.2.1 AMENAZAS DE PERSONAS (INTERNOS – EXTERNOS)

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.

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.

  1
- **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.

Un aspecto importante como parte de las políticas de Seguridad en las empresas es el hecho de seguir las siguiente recomendaciones:

- ✓ La creación de un compromiso del personal con las políticas propuestas por las organizaciones en las que se les haga firmar un acuerdo de cumplimiento a estas políticas (documento que contendrá en detalle los risks (riesgos) que deben evitar y las sanciones a las que estan sujetos en caso de incumplirlas).

- ✓ Capacitar constantemente a los usuarios por departamento, en base a boletines, e-mail, charlas, sobre el entorno actual de las tecnologías informáticas y el uso adecuado de los recursos informáticos dentro de la organización, asi como el el uso apropiado de Internet, etc.

- ✓ Los dos puntos anteriores en vista de una concientización en cuanto al correcto uso interno de la red y los recursos por parte del personal de la organización.

2.3 POLITICAS ORGANIZACIONALES

Se recomienda tomar en cuenta las siguientes medidas para deshacerse de documentación valiosa para la organización.

Hay cierta información a la cual suele llamársele “basura” corporativa (que incluye borradores de organigramas, manuales de computación, disquetes, impresos, notas manuscritas, memos, números telefónicos, notificaciones sobre asignación de proyectos y mucho más) material que puede allanarle el camino a un ingeniero social ávido de infiltrarse en las redes de las empresas. Para prevenirse de ataques, se aconseja:

- ✓ Ordenar la información según el grado de confidencialidad, y luego establecer procedimientos sobre cómo deshacerse de dicho material.

- ✓ Destruir la información clasificada antes de eliminarla. Se sugiere no utilizar destructoras de papel que lo cortan en tiras (ya que el documento puede ser reconstruido por un hacker con determinación y paciencia); es mejor optar por las que convierten el papel en una pulpa inutilizable. Borrar o inhabilitar los soportes de datos digitales (disquetes, discos Zip, CDs o DVDs con archivos, cintas removibles, discos rígidos viejos y otros medios de almacenamiento de datos) antes de descartarlos. Recuerde que borrar los archivos no es equivalente a eliminarlos.

- ✓ Controlar la selección de la gente que integrará las cuadrillas de limpieza, verificando cuidadosamente sus antecedentes cuando sea necesario.

- ✓ Recordar periódicamente a los empleados que presten atención a los tipos de papeles y materiales que desechan.

- ✓ Restringir el acceso a los depósitos de basura.

- ✓ Utilizar recipientes especiales para colocar materiales con información clasificada, y contratar a una compañía especializada en deshacerse de ellos (en caso de ser necesario).

2.3.1 A NIVEL FÍSICO

Se prohibe el ingreso y consumo de bebidas (todo tipo), alimentos y el tabaco en las proximidades de equipos electrónicos (cables de red, estaciones de trabajo, servidores, equipo de internetworking).

- ✓ Restringuir el acceso a los usuarios al áreade los Servidores, ingresando unicamente el Administrador de la red o algún usuario al que se le asigne el ingreso. Establecimiento de controles de acceso a la sala de equipos (especialmente donde se encuentran los servidores).

- ✓ Se prohibe el ingreso de dispositivos de almacenamiento y medios removibles a la organización (disquette, memorias, discos duros) para evitar el hurto de información o aplicaciones críticas de la organización.

- ✓ Definir cuotas de disco para las carpetas particulares de los usuarios que hay en el servidor.

- ✓ Prevenir el uso de la ingeniería social dentro de la organización concientización de los usuarios, implementar entrenamiento de los usuarios, cambios de passwords periodicamente).

- ✓ Es importante recordar que quienes tienen acceso físico a un equipo tienen control absoluto del mismo. Por ello solo deberian accederlo aquellas personas que sean estrictamente necesarios.

2.3.2 ANTE DESASTRES NATURALES

- ✓ Contar con sistemas de detección y protección de incendios en la sala de servidores y demás equipo de internetworking.

2.3.3 PARA LOS USUARIOS

- ✓ Prevenir el acceso a Sitios Web inapropiados.

- ✓ Prevenir o restringir el uso de aplicaciones P2P con los cuales los usuarios puedan compartir y descargar archivos que utilizan un gran ancho de banda (que salta de puerto en puerto) abriendo un medio para posibles ataques a la red .

- ✓ Limitar el uso de mensajeria instantánea ya sea por aol, icq, yahoo messenger, msn messenger, etc. Evitando la recepción y envío de información por este medio, como alternativa se puede permitir el uso de chats corporativos.

- ✓ 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.

- ✓ Prohibir o restringir el uso de cualquier wallpaper o papel tapíz esto es para prevenir imágenes que pueden ser consideradas ofensivas por algunos miembros del personal desde que comienzan a mostrarse en los monitores de

la compañía. Los empleados podrían utilizar screen savers ya definidos y habilitados en sus máquinas.

- ✓ Prohibir el acceso a sitios web inapropiados (según criterios de la organización).

- ✓ Prevenir los siguientes ataques: Denegación de Servicio (DoS), Denegación de servicio distribuida (DDoS), ataques de rastreo de tráfico y ataques de acceso no autorizado.

- ✓ Proveer conexiones seguras en la red permitiendo la confidencialidad e integridad de datos sensibles transmitidos atraves de conexiones remotas al utilizar una red pública.

- ✓ Optimizar los recursos y reducir los costes en una red valiéndose de Internet.

- ✓ Alertar en tiempo real sobre sucesos en la red para brindar respuestas de administración rápidas y óptimas ante cualquier cambio.

- ✓ Proveer servicios criptográficos de seguridad.

- ✓ Prever fallas en la red en caso de que el cortafuego falle, manteniendo activo el tráfico en la red y preservando las conexiones existentes.

- ✓ Manejar niveles de seguridad para los usuarios cuando estos se autentiquen en el Router, proporcionando métodos de acceso más seguros.

2.3.4 USO DE CLAVES DE ACCESO

- ✓ Todo usuario que tenga acceso a estaciones de trabajo o computadores personales, acceso remoto, o cualquier otro servicio dependiente de la red corporativa, utilizará claves de acceso personales, no compartidas, tanto para

acceder a la red, al Correo y a cada una de las aplicaciones que útilice en su trabajo.

2.4 POLÍTICAS TÉCNICAS

- ✓ Implementar URL (filtro de localizador de recursos uniforme), para prevenir que los usuarios navegen en sitios web inapropiados. Esto se ve efectivo solo si los usuarios están forzando su uso.

- ✓ Hacer uso de la técnica de TCP/Intercept, para prevenir de todo tipo de ataque DoS que se origina desde el exterior de un sistema através de la red, siendo: TCP, UDP e ICMP. Los protocolos en los que se basan las técnicas de saturación de paquetes o *flooding*.

- ✓ Utilizar Rate Limiting (Limite de tarifa), para prevenir ataques de tipo DDoS, ataques de inundación de tráfico, de manera que pueda limitarse el impacto de ataque a la red. Restringiendo el uso de ancho de banda para una categoria de tráfico específica.

- ✓ Valerse del uso de Reverse Path Forwarding (Reenvio de Trayectoria Reversa) para la prevención de Spoofing de direcciones IP, válido para tráfico Multicast y Unicast comparandose la entrada con las de la tabla de enrutamiento para determinar si el paquete es aceptado o descartado.

- ✓ Utilizar Black Hole para deshacerse del tráfico no deseado, proporcionando autenticación completa en el tráfico que entra y sale de la red alertando con mensajes en tiempo real, de manera que; se provean respuestas de manera rápida y segura ante posibles ataques que inestabilicen la seguridad de la red.

- ✓ Utilizar ACL's (Listas de Control de Acceso) para controlar el tráfico en la red, ya sea para permitir o denegar tráfico (dependiendo de las necesidades de la organización). Valiendose de las ACL estándar y extendidas.

- ✓ Implementar la técnica CBAC (Control de Acceso basado en Contexto), para proporcionar un control de acceso seguro por aplicación atraves de los perimetros de la red.

- ✓ Utilizar NBAR (Aplicación de Red basado en Reconocimiento) para clasificar el tráfico que pasa por la red, facilitando al administrador para que pueda rápidamente comprender qué porcentajes de los recursos de red son usados por las aplicaciones, gestionando asi el ancho de banda.

- ✓ Configurar una VPN (Red Privada Virtual), valiéndose de el uso de la autenticación, encriptación y el uso de túneles (encapsulación) para proveer conexiones mas seguras y permitir que la informacion viaje de manera integra, confidencial y segura.

  Estableciendo túneles virtuales entre dos puntos con la finalidad de optimizar los recursos de la red y reducir los costes al utilizar una sola línea para el acceso a Internet.

- ✓ Hacer uso de IDS (Sistema de Deteccion de Intrusos), para monitorear los eventos y vulnerabilidades que se van descubriendo a nivel de TCP/IP y de los servidores de red en busca de intentos de intrusión, de manera que se pueda alertar acerca de toda actividad sospechosa que sucede antes y después de un ataque.

- ✓ Implementar NAT (Traduccion de Direcciones de Red), principalmente para proteger la privacidad de las direcciones ip de la red interna y como mecanismo para 'extender' el rango de direcciones disponible en una red pudiendo dar acceso a muchos ordenadores con una sola IP pública.

- ✓ Utilizar PAT (Traslado de Direcciones de Puerto), para que teniendo las direcciones y puertos reales de las maquinas origenes y destinos, permita la entrega de paquetes al momento de aplicar la técnica de NAT.

- ✓ Hacer uso de IPSec (Protocolo de seguridad de internet), de modo que al habilitar los servicios criptograficos de seguridad en la red se permita la autenticación, integridad, control de acceso y confidencialidad pudiendo usarlo con cualquier protocolo IP sobre IPSec.

- ✓ Utilizar AP (Autenticación Proxy), para habilitar la posibilidad de definir políticas de acceso de seguridad por usuario, las cuales entran en funcionamiento en el momento en que los usuarios se autentican para acceder a la red.

- ✓ Configurar el método de Failover, de modo que; al existir una falla en el cortafuego primario el de reserva sea el que tome la actividad como si fuera el principal de modo que no se pierdan las conexiones existentes.

2.5 ESTRATEGIA DE SEGURIDAD

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

- La **Estrategia Proactiva** (proteger y proceder) o de 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.

2.6 RECOMENDACIONES EN EL MANEJO DE LA ADMINISTRACIÓN DE ACCESOS

1. Para el acceso a información de la red corporativa será necesario estar debidamente autorización 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 correcta el accesos a los usuarios de acuerdo al perfil autorizado.
4. En caso de que 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.

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 el fin de violar la seguridad de los sistemas.

7. Las cuentas bloqueadas podrán ser habilitadas nuevamente después que, el jefe inmediato envié una solicitud al administrador de dicha aplicación.

8. Si el empleado deja de trabajar por diferentes circunstancias los permisos de acceso a la red corporativa se cancelarán de inmediato.

9. 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.

CAPÍTULO 3. DESARROLLO DE ESTUDIO DE MERCADO

3.1 INTRODUCCIÓN

En la actualidad, son muchas las Empresas de diferentes rubros que poseen redes informáticas, para el logro de sus objetivos (ya sean estas pequeñas, medianas o grandes empresas), acoplando estas redes a sus necesidades y estando a la vanguardia con la tecnología; es por ello que se ven en la necesidad de implementar medidas de seguridad que garanticen la fiabilidad de la información.

Es importante mencionar que a nivel mundial las tecnologías informáticas (sean estas Software, Hardware no importando marcas, proveedores o creadores) han venido a revolucionar la manera de operar de las Empresas y por ello los procesos operativos y/o productivos de ellas.

Siendo las redes informáticas muy demandadas en la actualidad, parte de la investigación versa sobre un Estudio de Mercado de la Situación Actual de las Redes Informáticas en El Salvador y aspectos de seguridad que ésta conlleve.

Con dicho estudio, se pretende hacer un análisis de la manera en que las Empresas aseguran su información y de qué herramientas se valen para resguardar sus datos ante una gran variedad de ataques que existen hoy en día.

La expansión de las redes de computadores en los últimos años se considera que ha sido elevado, junto a esta situación su uso y aceptación. Por lo tanto, los riesgos de seguridad de información para las diversas Empresas que hagan uso de las redes informáticas, si éstas; no son enmarcadas en un contexto de seguridad idóneo.

3.2 PUNTOS A CONSIDERAR PARA REALIZAR LA ENCUESTA

- Sector al que pertenece la Empresa.
- Prioridad asignada para garantizar la protección de la información.
- Peligros considerados como más apremiantes por los que se ve afectada la red.
- Tipos y marcas de equipo internetworking que las empresas utilizan.
- Información de personas que realizan las configuraciones de dicho equipo.
- Proveedores del equipo.
- Inversiones monetarias realizadas hasta la fecha y fondos disponibles para la implementación de técnicas de seguridad.
- Tecnologías de seguridad que son utilizadas y permiten asegurar la información en las Empresas.

Tomando en cuenta cada uno de los puntos anteriores, se busca obtener un análisis real, demostrando la poca protección que tienen las redes de muchas organizaciones y por consiguiente el eminente peligro de su data. Además es importante hacer una cuantificación de la posibilidad de hacer uso de un Firewall utilizando un Router de la marca Cisco, brindando con ello un servicio y cubriendo las necesidades, que en este caso tienen que ver con la Seguridad de la Data de cada organización.

3.3 DISEÑO DE LA INVESTIGACIÓN

3.3.1 OBJETIVO GENERAL

- Identificar las tecnologías que utilizan las empresas para proteger sus redes de posibles ataques y la importancia que tiene el tema de Seguridad en cuanto a la protección de los datos.

3.3.2 OBJETIVOS ESPECÍFICOS

- Determinar la importancia que los Administradores de redes de computadoras otorgan al tema de seguridad Informática.
- Investigar y Determinar los diversos peligros que las empresas consideran como más apremiantes hoy en día por las cuales la seguridad en sus redes se ve mermada.
- Determinar la tendencia en los productos de internetworking y tecnologías de seguridad que se utilizan en la actualidad para el manejo de la información.
- Conocer la viabilidad y nivel de aceptación que tendría la técnica de utilizar un Router Cisco como Firewall.
- Presentar un estimado de la inversión monetaria que las Empresas han invertido hasta el momento en materia de seguridad y sus pretensiones económicas para el futuro.
- Cuantificar la necesidad de disponer del tipo de tecnología o servicio que se está proponiendo.

3.4 METODOLOGÍA

3.4.1 UNIDAD DE INVESTIGACIÓN

El Estudio de La Situación Actual en Seguridad de Redes Informáticas en El Salvador, ha sido aplicado a entidades que en el País son catalogadas como pequeñas y medianas (PYMES).

Para efectos de estudio, se establece como Pequeñas Empresas a aquellas que poseen una plantilla de personal entre cinco y cincuenta empleados. Por otro lado, Medianas Empresas son consideradas aquellas que cuentan con una plantilla de personal entre cincuenta y ciento cincuenta empleados.

La investigación se llevó a cabo a través de dos fases:

Fase de Exploración

En esta fase se realizó una exploración a fin de identificar aquellas empresas que utilizan equipo de internetworking y que además necesitan protegerse de diversos tipos de ataques, los cuales pongan en riesgo los datos. Para ello se investigó un total de 45 empresas a fin de determinar posibles candidatos para la investigación, enmarcando el estudio en un total de 31 empresas.

Fase de entrevista y recolección de la información mediante Encuesta

Una vez establecido el listado de las empresas, se procedió a realizar los contactos necesarios para gestionar una Encuesta y poder recolectar los datos de acuerdo a los objetivos específicos planteados.

Dado que uno de los objetivos de esta investigación era identificar a las empresas que de una u otra forma tiene la necesidad de proteger su información ante ataques externos. Dicho de otras palabras, empresas que protejan su red interna.

La Encuesta, la cual consiste básicamente, en realizar una serie de **preguntas** abiertas y cerradas que permiten sacar conclusiones para trabajar en base a ellas siendo la base para el alcance de los objetivos planteados.

Para el caso preguntas cerradas son las que brindan opciónes para responder (Si, no / Opción: A, B, C), y preguntas abiertas son las que dejan que las personas encuestadas respondan con mayor libertad (¿Por qué? / ¿Qué piensa al respecto?, etc).

La Encuesta se realizó al encargado de Administrar la Red en cada empresa y para ello se útilizó una guía de entrevista estructurada. Cabe mencionar que el medio utilizado para ello fue vía Web, en el cual se le proporcionaba a la persona un sitio Web a visitar y posteriormente responder las preguntas que ahí se presentaban.

Se diseñó una encuesta de 16 preguntas, siendo estas de selección múltiple y salvo en 4 preguntas que se determinaron de complementar, estando sujetas a la pregunta anterior y dependía de ésta, si sería contestada también.

Cabe mencionar que la encuesta fue elaborada en PHP teniendo para ello a disponibilidad un Servidor Web y la Base de Datos para la recolección y almacenamiento de los diversos datos; estos datos fueron administrados desde el mismo sitio, obteniendo un consolidado de la información obtenida.

3.4.2 DESCRIPCIÓN DE LA DEMANDA

En base a la información recopilada, se identificaron 31 empresas que utilizan equipo de internetworking para proteger su red interna ante una gran variedad de ataques que ponen en riesgo la información.

A forma de mantener cierta discreción, se ha agrupado a las empresas por sectores, dentro de los cuales se han considerado los siguientes:

- ONG´s
- Salud
- Gobierno
- Financiero
- Transporte
- Educación
- Tecnología
- Telecomunicaciones
- Servicios Varios

De estos sectores, quienes más implementan medidas de seguridad están: El Sector Tecnología, Telecomunicaciones y el Sector Financiero. Ellos asignan una prioridad extrema al momento de asegurar la protección de los Datos.

En cuanto a los peligros considerados como más apremiantes, se listan los siguientes: Spamming de Correo electrónico, Robo de Información y Abuso del uso de Internet. Para lo cual dentro de las tecnologías que se utilizan con mayor frecuencia, se pueden citar el uso de Antivirus y el Uso de Firewall tanto a nivel de Software y Hardware.

A nivel de equipo de Internetworking más útilzados están los Router y Switches administrables, los cuales son utilizados para proteger la red interna, utilizando técnicas específicas que garantizan la seguridad de los datos. Siempre en el tema de los Equipos, existe una gran demanda en el mercado actual por la marca Cisco, ya que del 100 % de las empresas entrevistadas, un 56 % hacen uso de equipo Cisco System.

Cuando se habla de equipo, no puede dejarse de lado el tema de Inversión que las empresas realizan en materia de seguridad. Refiriéndonos a presupuestos

destinados a proteger la red. Las cantidades de dinero son bastante variables, y éstas van desde los $ 1000 en adelante. Cabe mencionar que los niveles de inversión dependen del tamaño de la empresa, del tipo de información que manejan de la necesidad que se tenga de proteger los datos.

Ante el acelerado crecimiento, tanto de las tecnologías de seguridad como el de tipos de ataques, surge la necesidad por parte de las empresas de mantenerse protegidos optando por una gama de equipos y software de protección. Actualmente las grandes empresas optan por adquirir equipo comúnmente llamado “Appliances” los cuales tienen como misión dedicarse específicamente a la tarea para la cual han sido diseñados. Pero como el estudio ha sido orientado más que todo al tipo de pequeña y mediana empresa; para ello existen alternativas en el mercado de mantenerse protegido optando por diversos tipos de herramientas y tecnologías.

El mayor interés se centra a nivel de los Firewall como herramienta a utilizar dentro de las empresas. Estando como opciónes el adquirir un Firewall basado en Software, los cuales ante ciertos tipos de ataques se ven limitados, Firewall basados en Hardware implicando con ello una considerable inversión o el hacer uso de equipo ya existente en la empresa; tal es el caso de hacer uso de Firewall utilizando un Router.

El estudio nos muestra que un 38% está interesado en hacer uso de un Firewall independientemente de que tipo sea y del total de empresas entrevistadas un 10% estaría bastante interesada en implementar el uso de un Firewall utilizando Routers. Es importante recalcar el hecho de que esta última opción no es muy conocida y a pesar de ello se tiene un estimado de que del total
de empresas entrevistadas, 3 de ellas podrían hacer uso de esta solución de seguridad; dicho de otras palabras, existe cierto interés de utilizar el equipo existente dentro de las empresas, en este caso que los router puedan ser usados para fines de seguridad.

3.4.3 COBERTURA

Tanto el planeamiento y la ejecución de la encuesta fueron realizados en el periodo Abril – Mayo del presente.

Para su aplicación se consideraron aspectos como el directorio actual de las empresas y cuya muestra fue establecida en un total de 31 instituciones, las cuales están localizadas en la zona metropolitana de San Salvador, pero la mayoría de éstas poseen sucursales a lo largo y ancho del territorio Salvadoreño.
El siguiente cuadro muestra la cantidad de Empresas encuestadas, distribuidas por Rubro Empresarial:

SECTOR	**TOTAL**
ONG	3
Salud	0
Gobierno	4
Financiero	5
Transporte	0
Educación	2
Tecnología	7
Servicios Varios	2
Telecomunicaciones	5
Otros	3
Totales	31

Tabla 3. 1 Cantidad de empresas encuestadas por rubro empresarial

Dentro de la categoría de Otros según los datos obtenidos los Rubros Empresariales que se encuestaron fueron:
Sector:

- Avicultura
- Restaurante
- Call Center

3.5 JUSTIFICACIÓN DEL USO DE UN ROUTER CÓMO FIREWALL

En el mercado actual existe una diversidad de opciónes a utilizar para proteger el perímetro interno de una Red, variando aspectos como calidad, precio, funcionalidad, adaptabilidad, etc.

Estudios realizados muestran la aceptación que tiene Cisco en el mercado Salvadoreño, aunque es de aclarar que se tienen muchas otras opciónes a tomar en cuenta y las cuales son herramientas complejas y robustas en cuanto a proteger y brindar seguridad en el perímetro de una red. Para ello se pueden citar los siguientes:

- Firewall Fortinet
- Firewall PIX de Cisco
- Firewall CheckPoint
- Firewall utilizando Routers

Los Firewall como tal en la actualidad tienen bastante aceptación y demanda; en el mercado Salvadoreño se observa que un porcentaje considerable hacen uso de un Firewall o tienen proyectado implementar esta tecnología.

Otro aspecto de relevancia es el nivel de conocimiento que se tenga en cuanto a las opciónes que se tienen actualmente en el mercado.

El hacer uso de un Router Cisco como Firewall para proteger una red, es una opción más que se tiene como herramienta o tecnología. Existe un detalle muy importante y es que pocos saben que la tecnología propuesta puede implementarse y adaptarse a las necesidades que existen al querer proteger una red.

Es por ello que hasta cierto punto el nivel de aceptación depende del nivel de conocimiento que se tenga de dicha tecnología. El estudio para el caso presenta

datos aceptables en cuanto a la posible implementación de un Router como Firewall ya que a pesar del poco conocimiento en el área, se sabe que entre 3 y 5 empresas estarían en la disponibilidad de hacer uso de dicha tecnología.

Es de tomar en cuenta que el prototipo que se presenta va dirigido a empresas catalogadas como pequeñas y que el número de usuarios es acorde al nivel de la empresa. También al igual que muchas otras opciónes en el mercado, haciendo uso del prototipo propuesto, se tienen tanto ventajas como desventajas. Se consideran aspectos relacionados al costo de equipo, costo de implementación, requerimientos, configuraciones de red, escalabilidad, etc.

3.6 OPCIONES EN EL MERCADO DE IOS FIREWALL DE CISCO

Actualmente en el mercado existe una diversidad de opciones a elegir en cuanto a tecnologías de seguridad orientadas al tema de Seguridad de Redes.

Cabe mencionar que la elección de estas tecnologías depende de diversos factores, tales como: tamaño de la empresa, topología de la red, equipo o hardware disponible en la estructura de red, disponibilidad económica, etc.
A continuación se mencionaran algunas, las cuales en determinada situación pueden ser consideradas como alternativas a implementar:

Fortinet: FortiGate - La nueva generación de Antivirus - Firewall tiene como objetivo la protección de red en tiempo real demandada actualmente en el mercado. El primer gateway de protección en tiempo real con antivirus basado en ASICs e IDS y además filtrado de URL.
FortiGate Antivirus Firewall, desarrollada por Fortinet, es la primera gama de aplicaciones de alto rendimiento para la protección de redes en tiempo real. Se trata de plataformas que combinan hardware y software para ofrecer antivirus, filtrado de contenidos web y de email, cortafuegos de inspección detallada, IPSec VPN, detección y prevención de intrusiones y funciones de perfilado de tráfico. Asimismo,

FortiGate detecta y elimina las amenazas que provienen de los contenidos email y del tráfico web en tiempo real, todo ello sin reducir el rendimiento de la red.

Fortinet ofrece alto rendimiento, construido específicamente para ser gestionado remotamente y sin pérdidas de rendimiento.

Carácterísticas:

- Antivirus/protección ante gusanos para tráfico de correo electrónico, Web y transferencia de archivos **(con certificación ICSA)**
- Firewall **(con certificación ICSA)**
- VPN **(con certificación ICSA)**
- Detección de intrusiones en la red **(con certificación ICSA)**
- Prevención de intrusiones
- Filtrado de contenido Web basado en URLs y palabras clave
- Filtrado de contenido de correo electrónico
- Conformación de tráfico (traffic shaping)

SonicWALL PRO: Dispositivo de seguridad de Internet ofrece:

- Protección de cortafuegos y concentración VPN económicos y de clase empresarial
- Soporte integrado para servicios de seguridad SonicWALL, inclusive antivirus y filtrado de contenido reforzados
- Ampliación opcional a SonicOS Enhanced, para continuidad del negocio y flexibilidad de configuración
- Gestión central basada en Web mediante el galardonado Sistema de Gestión Global de SonicWALL

WatchGuard: La línea Firebox X Edge de WatchGuard está diseñada para ser el punto perfecto de terminación de la VPN con modelos Firebox X, ampliando las capacidades de este modelo según las actuales necesidades de seguridad mediante una actualización por licencia. La línea Firebox X Edge ofrece una seguridad superior

en las redes gracias a sus características de firewall y VPN, a su fácil configuración con el software de gestión y el servicio de actualización, diseñado para aumentar de forma paralela al crecimiento de la empresa y para conocer las necesidades de seguridad de la misma. Todos los modelos Firebox X Edge se integran con la línea de dispositivos de seguridad integrada Firebox X, proporcionando una seguridad completa a las organizaciones que están distribuidas geográficamente.

Esta nueva familia integra numerosas funciones de seguridad en un único dispositivo y combina firewall de inspección de paquetes stateful dinámicos, VPN, soporte DNS dinámico, seguridad inalámbrica, software VPN IPSec para usuarios móviles, antivirus de sobremesa y WAN a prueba de fallos, todo dentro de una arquitectura de seguridad inteligente por niveles de aplicación.

Características de Firebox X Edge: Firebox X Edge protege las redes corporativas proporcionando conexiones seguras con las oficinas remotas, que se encuentran fuera del perímetro de seguridad ofrecida por el dispositivo Firebox X a la oficina central. Combinado con el dispositivo Firebox X, el nuevo Firebox X Edge proporciona:

- · Protección de los túneles VPN y de la oficina central
- · Seguridad de la red más completa
- · Software VPN IPSec para usuarios móviles
- · Sencillez de configuración y gestión
- · Gestión centralizada
- · Modelo actualizable mediante licencia para un servicio completo
- · Asistencia experta y soporte con el servicio LiveSecurity
- · Ahorro de tiempo y dinero

CISCO: Firewall **PIX** son dispositivos los cuales llevan un sistema operativo no UNIX muy seguro y de tiempo real. Una aplicación dedicada a la gestión de la máquina que permite evitar los bugs, backdoors y demás problemas de seguridad típicos.

Características:

Adaptive Security Algorithm: El algoritmo de seguridad ASA es el corazón del firewall PIX. ASA esta basado en estado y orientado a conexión.

Cut-through Proxy: PIX utiliza un método denominado *"cut-through proxy"* que permite verificar si los usuarios tienen permisos para ejecutar una aplicación TCP o UDP antes de llegar a la aplicación, *es decir, verifica a los usuarios en el mismo firewall.*

Filtrado URL: El firewall PIX verifica las peticiones URL salientes contra las políticas de seguridad definidas en el servidor UNIX o NT *(WebSense)*.

- El PIX permite conexiones basándose en las políticas de seguridad.
- La carga no esta situada en el PIX sino en una *maquina separada que lleva a cabo el filtrado URL.*

Opción de Failover/Hot Standby Upgrade: La opción de failover nos provee de una gran seguridad y elimina el caso de que en caso de que falle el PIX la red se quede sin funcionar.

Si un PIX funciona incorrectamente, o si están configurados incorrectamente, automáticamente el trafico pasa al otro PIX.

PIX NAT: ¿Qué es NAT? La característica "Network Address Translation (NAT)" trabaja sustituyendo, o traduciendo, direcciones de hosts en la red interna con una "dirección global" asociada con una interfaz externa.

Esta característica protege las direcciones de los hosts internos de ser expuestas en otras interfaces de red

PIX PAT: Significa "Port Address Translation". Puede ser configurado para que nuestro rango de IP logre direccionarse a los diferentes números de puerto TCP a una única IP. PAT puede ser usada en combinación con NAT

Los firewall PIX incorporan la última tecnología en seguridad:

- Inspección basada en el estado *(stateful inspection)*
- VPNs basadas en IPSec y L2TP/PPTP
- Filtrado de contenidos
- Detección de intrusos integrada

En el núcleo de la familia de Firewall PIX tenemos el algoritmo de seguridad ASA (Adaptive Security Algorithm) que mantiene aseguradas perimetralmente las redes controladas por los Firewalls.

La inspección de la conexión basada en el estado, en la que se usa el diseño ASA, permite crear flujos de sesión basándose en la dirección origen y destino, números de secuencia TCP (no predecibles), números de puerto y banderas TCP adicionales.

Check Point: SmartDefense es un producto que permite a los clientes configurar, imponer y actualizar defensas contra ataques a la red y aplicaciones. SmartDefense, que va incluido en FireWall-1®, protege activamente a las organizaciones frente a los ataques de red y aplicaciones mediante el empleo de la tecnología patentada Stateful Inspection y la innovadora tecnología Application Intelligence de Check Point.

Características del producto:

- Bloquea los ataques a las aplicaciones y la red según tipo y clase
- Actualizaciones de seguridad en línea: mantiene las defensas en estado óptimo
- Integración total con FireWall-1
- Registros con información detallada sobre los ataques, en tiempo real.

V*entajas del producto:*

- Seguridad integral de red y aplicaciones
- Fácil configuración de las defensas contra ataques
- Garantiza que todos los sistemas de defensa contra los ataques estén actualizados y sean coherentes en todo el entorno de seguridad.

Otras Soluciones:

Juniper Networks: *Las soluciones Juniper* integran varias tecnologías de seguridad y se presentan en dispositivos optimizados, basados en hardware y personalizados para garantizar las tareas que llevan a cabo. Entre las tecnologías básicas destacan: Firewall, VPN, Denegación de Servicio, Prevención de Intrusiones.

RSA Security: Los productos emplean tecnología token y smartcard, para el control de acceso software y/o hardware y autentificar la identidad de un usuario que accede a la red o a las fuentes de información. Proporciona a su vez soluciones de emisión y gestión de certificados digitales.
RSA Security permite realizar transacciones electrónicas proporcionando acceso seguro y proteger la información de la red, sistemas, aplicaciones y todas aquellas iniciativas de comercio electrónico.

NOKIA: Las soluciones de seguridad en **Internet** de **Nokia** combinan la tecnología de IP en Red de Nokia con las aplicaciones líderes en seguridad FireWall-1/VPN-1de Check Point, RealSecure de ISS. A través de estos partners **Nokia** proporciona dispositivos de alto rendimiento y fiabilidad que cubren todas las necesidades en materia de seguridad.

Websense: produce software para la administración y control de accesos corporativos a Internet. Su solución de filtrado de Internet administra, supervisa e informa acerca del uso de Internet por parte de los empleados.

Internet Security System: ISS proporciona soluciones para analizar las vulnerabilidades en redes, sistemas y bases de datos y para detectar y detener

intrusiones en tiempo real, tanto a nivel de red como de host. Ambas líneas de soluciones permiten evaluar y minimizar el riesgo en la seguridad de los sistemas de infraestructura de cualquier tipo de organización.
Los Appliances **Proventia** son dispositivos que automáticamente bloquean ataques, código malicioso y tráfico indeseado; además de preservar el ancho de banda y la disponibilidad de la red. Bloquea DoS, permite sustituir firewalls internos

CipherTrust: El exitoso dispositivo de seguridad de correo electrónico y anti-spam de CipherTrust proporciona tecnologías avanzadas de seguridad de correo electrónico y filtrado de spam para que las organizaciones puedan combatir de una manera más efectiva el spam, los virus, la modalidad de robo de información personal conocida como phishing, las negaciones de servicio y otras amenazas a la seguridad del correo electrónico.
Características de IronMail:

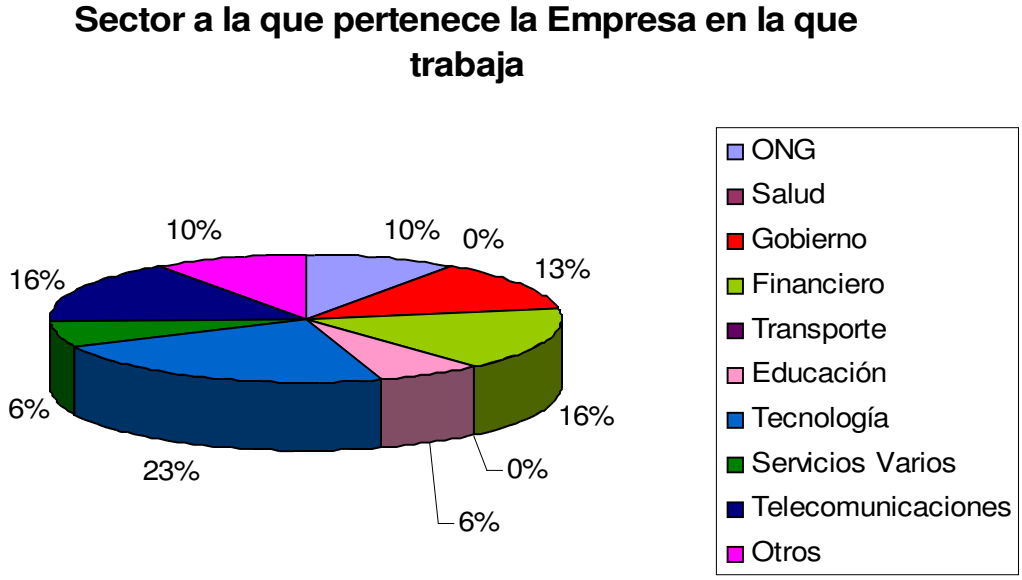
- Antivirus en el Gateway
- Protección de correo Spam
- Encriptación, Envío de mensajes seguros, Privacidad en el envío de mensajes
- Previene de Hackers, Intrusos, Denegaciones de Servicio, Firewall de correo.
- Permite políticas de correo

S-Box Defender: La Plataforma de Servicios de Seguridad S-box defender, cosiste en un dispositivo plug-and-play de fácil instalación, sin necesidad de conocimientos técnicos y que no requiere mantenimiento, cuya finalidad es la de proteger la conexión a Internet a través de línea telefónica, ADSL o cable.
Se trata de un appliance para:

- Proteger la privacidad de datos
- Mantener la integridad del PC y de la red
- Fitrar contenidos inapropiados (control de URLs)
- Detener virus
- Asegurar la vía de acceso a cualquier red corporativa.

3.7 GRÁFICOS Y RESULTADOS OBTENIDOS EN LA ENCUESTA

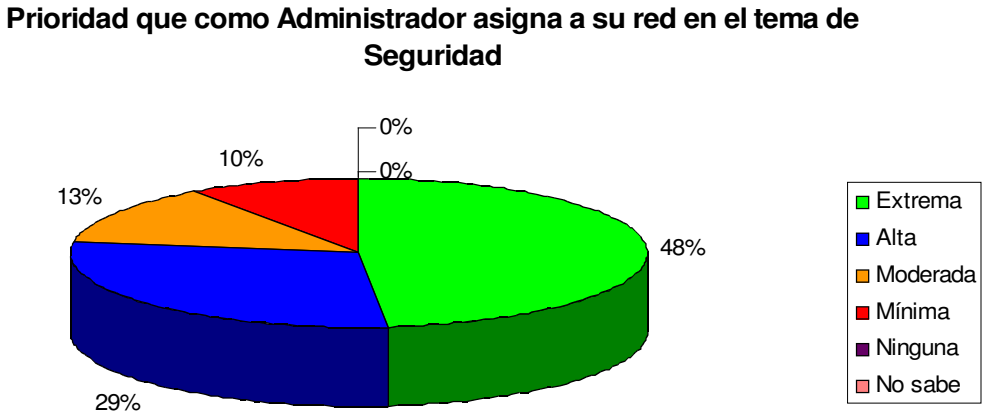
1. ¿A qué sector pertenece la empresa en la que usted trabaja?



Según los datos obtenidos en este pregunta la presencia de las Empresas por área esta distribuida de la siguiente manera:

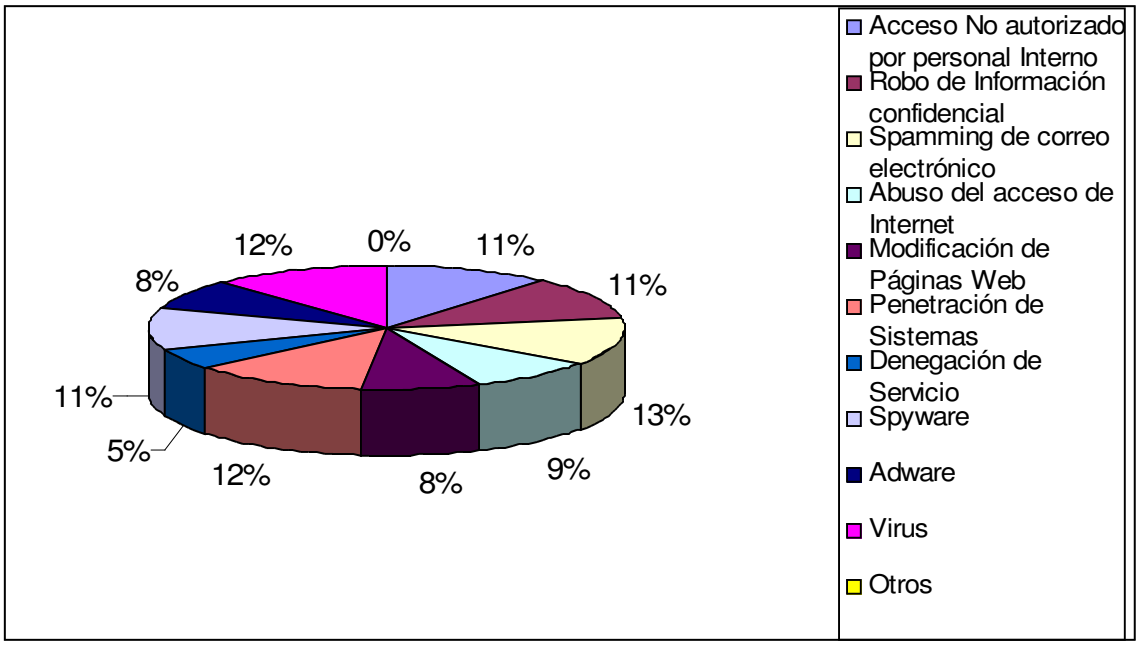
- El 23% lo enmarca el Sector de Tecnología.
- El 16% lo constituye el Sector de Telecomunicaciones.
- Otro 16% esta formado por el Sector Financiero.
- En el 13% se ubican Empresas que forma parte del Gobierno.
- Un 10% lo constituyen las ONG.
- El otro 10% corresponde a Otros (Encuestando a Empresas del Sector: Avicultura, Restaurante y Call Center).
- Un 6% lo integra el Sector de Servicios Varios.
- El 6% restante lo conforma el Sector de Educación.

3. ¿Qué Prioridad en el tema de Seguridad, asigna (ría) usted como Administrador en su red para asegurar la protección de los Datos?



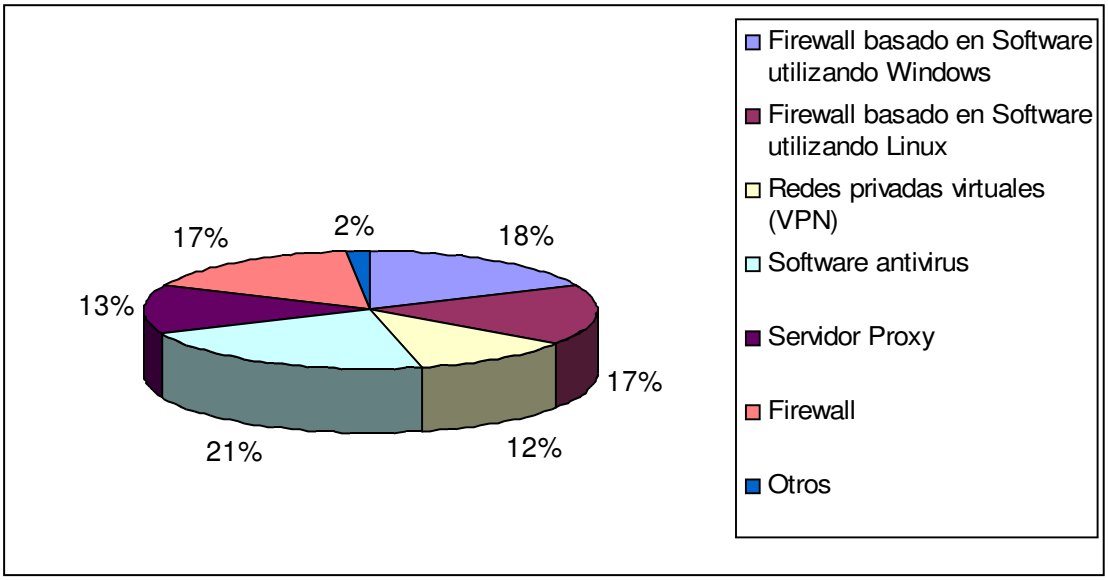
- En esta pregunta los Administradores de la seguridad de la red en un 48% aseguran que la prioridad que le asignan al tema de seguridad de la información es de carácter Extrema, las empresas que poseen este nivel de seguridad son aquellas dedicadas al área de Tecnología y Financiero.
- Por otro lado en la categoría de Alta lo abarca un 29% posicionándose en este sector Empresas del rubro: ONG, Gobierno y Telecomunicaciones.
- Dentro de un rango del 13% se encuentran las Empresas que consideran este tema Moderadamente perteneciendo a este, Empresas del sector: Educación y Otros.
- En un 10% se encuentran aquellas que consideran el tema de la seguridad como una prioridad Mínima, encontrándose en esta, Empresas que pertenecen al sector: Servicios Varios.
- En 0% se encuentra la categoría de Ninguna y No sabe, en la cual no fue enmarcado ningún Rubro Empresarial.

4. ¿Qué considera la organización como sus peligros más apremiantes?



- Un 12% de las Empresas consideran que la Penetración de Sistemas, el Spamming de correo electrónico y los virus son los peligros que les pueden afectar.
- El 11% considera que el robo de información confidencial y el acceso no autorizado por personal interno son de los peligros más apremiantes por los que se pueden ver afectados.
- El 9% de las Empresas opinan que el Abuso del acceso a Internet es un peligro latente.
- El 8% considera que el Spyware les afecta.
- Mientras que el 7% consideran al Adware como un peligro potencial.
- Por otro lado el 6% considera que el Fraude Financiero por el que se ven afectados.
- Un 5% consideran que la Modificación de Páginas Web y la Denegación de Servicios es un peligro palpable.
- Mientras que un 3% consideran al Fraude Telefónico como un peligro que les puede afectar.

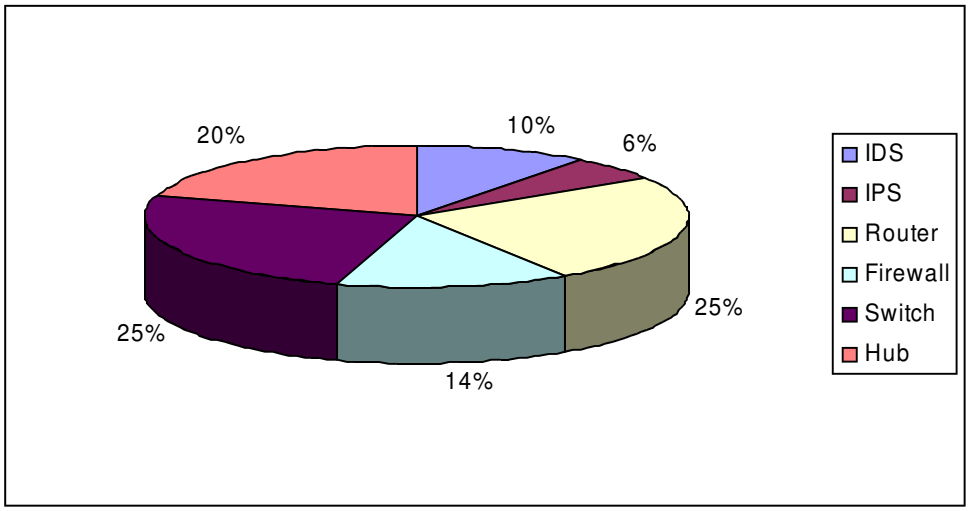
6. Tecnologías de seguridad que utilizan actualmente para asegurar la información de su empresa.



Existen diferentes tecnologías que se pueden implementar en las Empresas para asegurar la información que estas manejan, a continuación se presenta una clasificación de tecnologías que son las que utilizan con mayor frecuencia:

- El 21% afirman que utilizan Software Antivirus para protegerse de cualquier ataque de virus.
- Un 18% utilizan Firewall basado en Software utilizando Windows.
- Por un lado un 17% dice que utilizan Firewall para protegerse de cualquier amenaza externa a la organización.
- Mientras que el otro 17% emplean Firewall basado en Software utilizando Linux.
- Un 13% utiliza Servidor Proxy para protegerse de cualquier amenaza externa a la organización.
- Un 12% recurren a las Redes Privadas Virtuales (VPN).
- Un 2% se encuentra en la categoría de otros lo cuales describieron que utilizan PIX Cisco (Firewall Hardware), SpamKiller (protección contra spam (Linux)), Control de acceso al equipo y contraseñas, VLAN (Virtual Local Área Network)

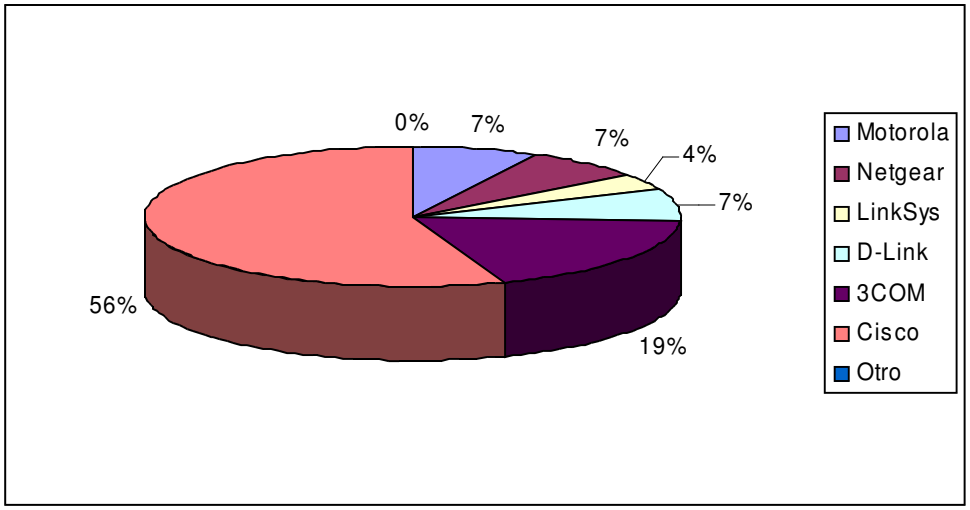
8. ¿Qué equipo de internetworking posee en su organización?



El porcentaje de Equipo de Internetworking que poseen las Organizaciones se detalla a continuación:

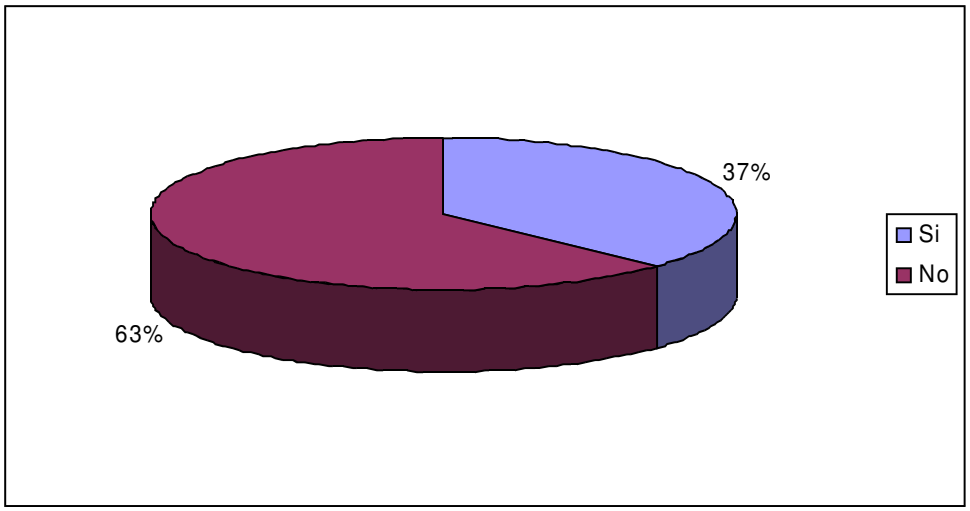
- Un 25% de las Empresas detallaron que utilizan Router, Switch implementados en su red de computadoras y asegurar los datos de la organización.
- Un 20% utilizan Hub en sus redes.
- Por otro lado el 14% afirma que utilizan Firewall.
- El 10% implementa IDS.
- Mientras que un 6% utilizan IPS.

9. ¿Si usted utiliza Router, éste que marca es?



- El siguiente gráfico muestra que de las Organizaciones que utilizan Router ***el 56% se inclinan por la marca Cisco.***
- Un 19% prefiere la marca 3COM para el enrutamiento de los datos.
- Mientras que un 7% opta por la marca Motorola, Netgear y D-Link para trabajar en su red.
- El 4% se inclina por trabajar con LinkSys.

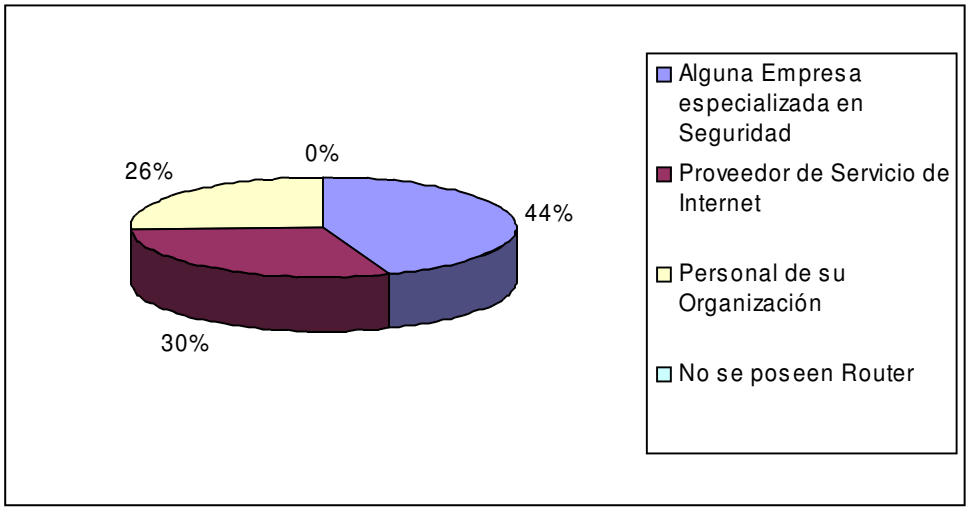
10. ¿El router es arrendado por algún Proveedor de Equipo?



Según los datos presentados en este grafico:

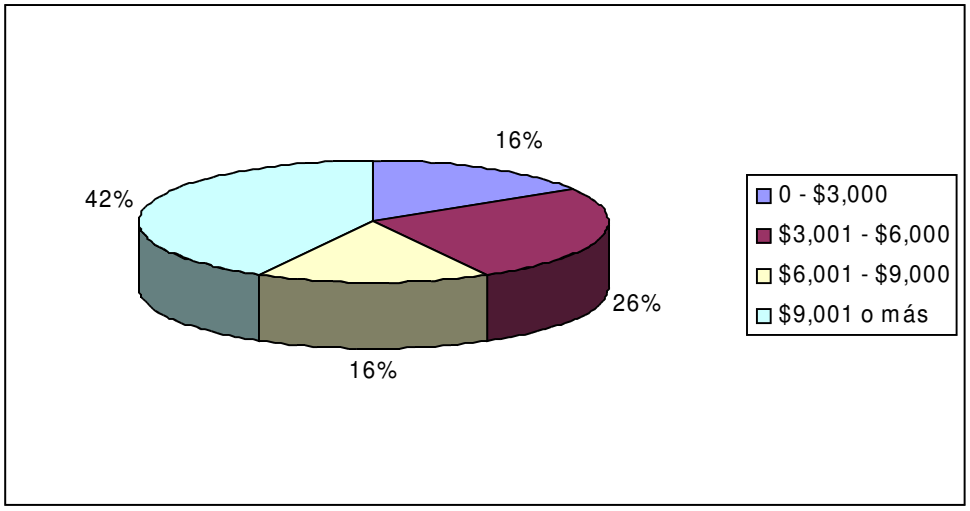
- Un 37% respondió afirmativamente en cuanto a que, el Router que poseen en su Organización es arrendado por algún Proveedor de Equipo.
- Mientras que un 63% indico que el Router que poseen en su Organización no ha sido arrendando.

11. ¿Quién realiza la configuración de su Router?



- El 44% contrata a Empresas especializadas en seguridad de redes para la configuración de los router.
- El 30% de la configuración de los Router la realiza el Proveedor de Servicio de Internet.
- Por otro lado el 26% de las Empresas, indican que la configuración la realiza personal de su organización ya que poseen empleados capacitados para realizar esta actividad.

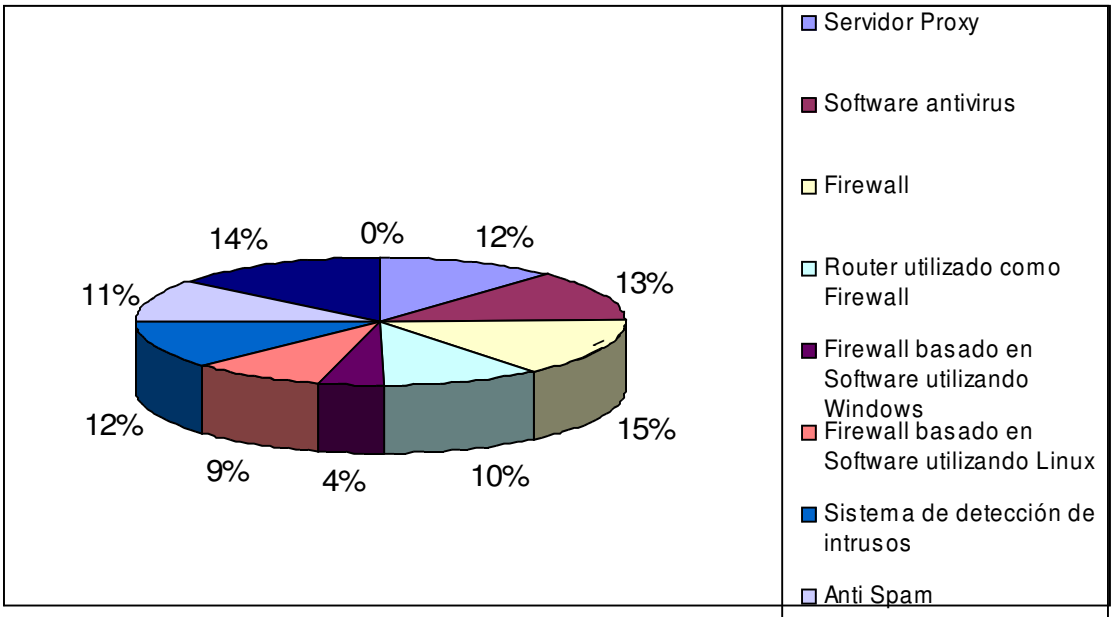
12. ¿Cuál ha sido la inversión monetaria hasta la fecha en materia de seguridad?



En el gráfico anterior se muestra la inversión que las Organizaciones han efectuado en un periodo de cinco años en materia de Seguridad, obteniendo los siguientes valores (Cantidades aproximadas):

- Un 42% afirman que han realizado una inversión monetaria de $9,001 o más.
- El 26% catalogan que han efectuado una inversión entre un rango de $3,001 o $6,000.
- Un 16% enfatizan que su inversión realizada oscila en un rango de $6,000 - $9,000.
- Mientras que otro 16% mencionaron que la inversión realizada fluctúa entre $0 - $3,000.

13. De las siguientes tecnologías, ¿cuáles estaría interesado en implementar?



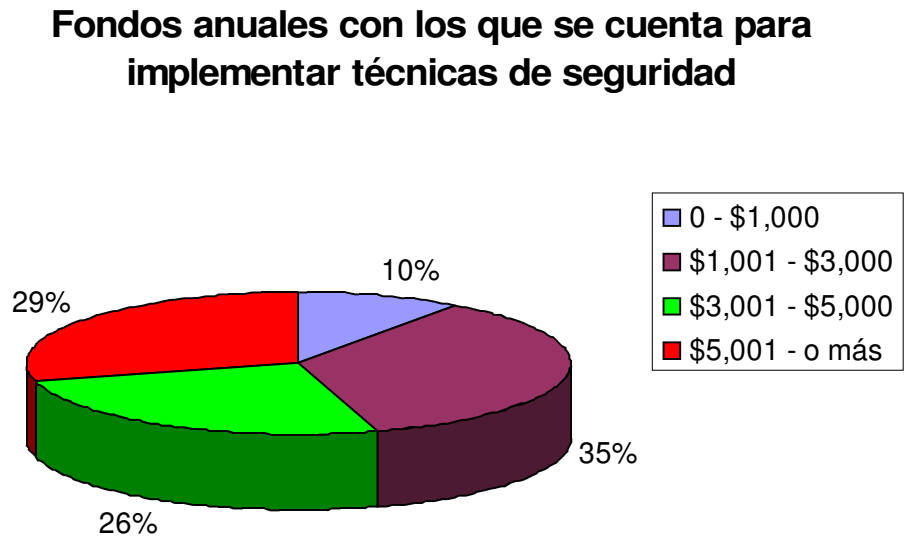
En el Mercado Informático existen en la actualidad, diferentes tecnologías que se podrían utilizar para asegurar la información, por lo que se puede observar en el siguiente gráfico las Empresas se muestran interesados en utilizar mas de una tecnología para proteger sus redes. Entre las tecnologías que, los usuarios consideran como posibles a implementar, según los datos obtenidos están:

- El uso de Firewall con un 15%.
- La utilización de Redes Privadas Virtuales (VPN) con un 14%.
- La preferencia por los Software Antivirus con un 13%.
- La implementación de Servidores Proxy y los Sistemas de Detección de Intrusos con un 12%.
- Un 11% se inclina por implementar Anti Spam.
- Un 10% estaría interesado en adquirir Router utilizado como Firewall.
- Mientras que un 9% elegirían usar Firewall basado en Software para Linux.
- Mientras que el 4% utilizan Firewall basado en Software para Windows.

15. ¿Qué equipo de internetworking utilizaría para proteger su organización de posibles ataques externos?

- La mayor parte de las Empresas consideran que el equipo con mayor fiabilidad para asegurar los datos de su empresa son los Firewall, el porcentaje que considera esta como la mejor opción es el 28%.
- Un 22% considera que una de las mejores opciónes es implementar un IDS e IPS para la protección de los datos.
- El 15% considera que la utilización de Switch es una buena opción para segmentar su red interna de tal forma que no existe comunicación entre departamentos.
- Mientras que el 13% utilizarían Router como la mejor opción para protegerse de posibles ataques externos.

16. ¿De cuanto son los fondos anuales con los que cuenta, para implementar algunas de las técnicas de seguridad antes mencionadas?



A continuación se muestra el total de la inversión que las Empresas esperan realizar en el siguiente año, para proteger la información que poseen: (Cantidades aproximadas):

- Un 35% detallan que pretenden realizar una inversión monetaria de $1,001 - $3,000.
- Mientras que el 29% proyectan invertir entre un rango de $5,001 o más.
- Por otro lado un 26% enfatizan que planean invertir entre $3,001 - $5,000.
- El 10% mencionaron que prevén invertir realizada fluctúa entre $0 - $1,000.

3.8 CONCLUSIONES DEL ESTUDIO DE MERCADO

A pesar del alto conocimiento que tengan los Administradores de Redes de algunas organizaciones, es importante enfocarse en que unas cuantas consideran como mínima y moderada la prioridad que le dan al tema de Seguridad por lo que se considera, se tiene que dar más énfasis al respecto en cada una de las instituciones encuestadas. Así mismo, dentro de los puntos más relevantes de la encuesta se ha podido observar que el 48% de las instituciones encuestadas consideran que la importancia de asegurar los datos de las empresas es extrema, estas instituciones son aquellas que se encuentran en el sector de tecnología y financiero.

Por otro lado, se puede observar como los Administradores de Red tienen bien claro los peligros mas apremiantes por los que pueden verse o se han visto afectados en un momento determinado y es evidente que son varias las opciónes a considerar.

En contra parte, los encuestados mencionaron las diversas tecnologías de seguridad que implementan actualmente en sus Empresas, en este punto es palpable la combinación de herramientas que los Administradores de Red hacen, para salvaguardar los datos en su organización, dentro de esta categoría mencionaron como tecnologías adicionales que suelen implementar: PIX Cisco (Firewall Hardware), SpamKiller (protección contra spam (Linux)), Control de acceso al equipo y contraseñas, VLAN´s.

De igual manera, en la pregunta relacionada al Equipo de Internetworking que las Organizaciones poseen los datos obtenidos revelan que las Empresas no solo se enmarcan en un área de la tecnología, y que por el contrario; se valen de diversos recursos para obtener mayores beneficios en el desempeño de sus redes.

Dentro del marco que compete al desarrollo de este Estudio de Mercado se da a conocer la preferencia de los Administradores en cuanto a marcas de Router se

refiere y es evidente de que estos se inclinan por la marca CISCO, así también; quienes poseen Router detallaron que en la mayoría de los casos el equipo es arrendado por el Proveedor de Servicio, así como; las configuraciones necesarias en la mayoría de los casos son realizadas por personal de la misma Organización.

Dando a conocer un estimado de la inversión que han realizado en las Organizaciones, en un período de cinco años en materia de seguridad, mencionando que el 45% de los encuestados ha realizado una inversión entre $3,001 - $5,000, el 39% entre $5,001 – o mas, mientras que el 10% de $0 - $1,000 y el 6% restante entre $,1001 - $3,000.

Analizando posibles tecnologías que en la Organizaciones podrían ser implementadas, de una gama que el Mercado ofrece en la actualidad, evaluando el hecho que los Administradores no se basan solo en una tecnología sino que suelen combinarlas para obtener mejores resultados ajustándose mejor a las necesidades en la Red. Como dato importante a mencionar se observa la preferencia de los usuarios en la implementación de Firewall y las Redes Privadas Virtuales.

Así también, tomando en cuenta la gama de posibilidades que les ofrece el Mercado el equipo de internetworking que podrían implementar dándole mucha importancia a lo que son el uso de los Firewall, IDS e IPS, no distando mucho de las que usan hoy en día.
Se hizo un análisis de la inversión (aproximada) con la que cuentan anualmente para realizar inversiones en materia de seguridad, algunas de las Organizaciones suelen mantener un parámetro de inversión ya que algunas poseen en la mayoría equipo propio, mientras que otro buen porcentaje suele arrendarlo.

En el mercado, existen actualmente una diversidad de tecnologías y herramientas de las que se valen los usuarios para proteger ante todo ataque el perímetro de su red y salvaguardar la integridad de su información. Conviene mencionar la importancia que se le da, al uso de una combinación de herramientas para lograr tal objetivo en las Empresas, ya que hoy en día no basta con solo tener un Firewall y garantizar la

seguridad en la red. Por lo que se ha determinado y se recomienda altamente que todas las pequeñas y medianas empresas deben tener una solución de seguridad en Internet.

Las actuales soluciones de seguridad requieren varias capas de protección para los diversos tipos de amenazas que afrontan las redes en la actualidad. Los firewalls están diseñados para alejar a los hackers al "cerrarles" básicamente las puertas de la red informática. Aunque los atacantes son más sofisticados y encuentran métodos más novedosos y rápidos de propagación, algunos ataques inevitablemente pasaran por el firewall, aunque no por la ruta de los IDS. La tecnología IDS funciona con el firewall de la red, sistema de failover, control y detección de vulnerabilidades aplicando diferentes técnicas para brindar máxima protección, las VPN, la implementación de NAT y PAT, asi tambien una autenticación de usuarios mediante AP, con la finalidad de reforzar las funcionalidades de administración de seguridad mediante la protección de todas las capas de la red.

Con el estudio realizado se han obtenido diversos indicativos que demuestran lo que se espera de una herramienta de protección en el perímetro de la red; al igual queda muy claro, que lo más importante a proteger son los datos de las empresas ante los ataques que existen.

Es por ello que se propone una opción más para la protección de los datos. Una herramienta que logre aplicar filtros de tal forma que se evite en gran manera los ataques que se podrían sufrir si no se tuviese nada para protegerse.

Con el prototipo de Firewall propuesto se pretende cubrir las necesidades de protección que requieren las empresas. También se pretende dejar muy en claro que se trata de una alternativa de protección, la cuál para tomarse en cuenta y llegarse a implementar requiere de un previo estudio de diversos factores a los cuáles va atado el buen funcionamiento del prototipo.

3.9 CASO PRÁCTICO. PROBLEMA A RESOLVER

El caso se aplica a empresas que tienen que hacer uso de Internet como medio de comunicación para efectuar sus transacciones de información. Además estas empresas tienen sucursales a lo largo y ancho del territorio nacional; también tienen como características que sus redes son relativamente pequeñas, estas oscilan entre 10 y 15 host por Agencia o Punto. En la central se poseen ciertos servidores de los cuales las sucursales acceden a la información contenida en éstos.

El problema principal radica en que tienen que compartir información a través de un medio el cual se cataloga como Inseguro (Internet), para lo cual surge la necesidad de contar con una herramienta que les permita estar protegidos tanto internamente como en el intercambio de datos que realicen.

El ejercicio que se propone es a nivel de 1 empresa que tiene un punto central y una sucursal, la cual necesita constantemente tener comunicación en cuanto a transmisión de datos ya que en el punto central se poseen servidores los cuales publican las aplicaciones para el funcionamiento los sistemas que manejan internamente.

Actualmente ésta información viaja a través de Internet corriendo el riesgo de que ésta sea interceptada. Además cada uno de los usuarios posee salida a Internet y por el momento no tienen ninguna herramienta que los proteja ante posibles ataques provenientes del exterior.

Ante la problemática presentada anteriormente se propone hacer uso de un Firewall utilizando Router Cisco, específicamente el modelo 1750 el cual es muy versátil y permite ser configurado como Firewall para la protección del perímetro de la red.

El cual incluya una serie de configuraciones adicionales a las que tiene normalmente un Router como tal, con el objetivo de que funcione como Firewall para la protección de la red.
Entre las configuraciones que se implementarían están las siguientes:
VPN: con la cual se pretende formar una vía segura por medio de la cual la información viaje entre las empresas de manera cifrada, garantizando con esto la integridad de la información.

Autenticación de Usuarios: con esto se pretende que solo personal autorizado y propio de la empresa puedan tener acceso a los recursos que se tienen en la red.

Protección ante ataques de Denegación de Servicio: con esto se busca garantizar la conectividad entre ambos puntos de la red. Como se sabe actualmente existen ataques cuyo propósito es el de hacer lo menos eficiente posible la comunicación, hasta tal punto que la conexión falla.

Redundancia o Failover: con el propósito de que siempre exista una vía de respaldo en cuanto a conectividad se refiere.

Para la aplicación de cada una de las configuraciones, se deben tener ciertas políticas donde se especifique qué es lo que se quiere permitir, qué es lo que se desea denegar y de qué se pretende proteger. Todo con el único objetivo de estar protegido ante cualquier eventualidad.

CAPÍTULO 4. IMPLEMENTACIÓN DEL FIREWALL

4.1 TIPOS DE ATAQUES [8]

4.1.1 FUENTES DE ORIGEN DE LOS ATAQUES DOS / DDOS

Los ataques de denegación de servicio suelen tener varios orígenes, lo que complica la posibilidad de mantener un control efectivo sobre todos los recursos o servicios ofrecidos. No obstante, los distintos orígenes pueden agruparse en:

1. **Usuarios legítimos o internos:** Este grupo se subdivide en aquellos usuarios poco cuidadosos que colapsan el sistema o servicio inconscientemente (por ejemplo la persona que llena el disco duro del sistema bajando archivos de música), usuarios malintencionados (aquellos que aprovechan su acceso para causar problemas de forma premeditada) y usuarios ladrones que utilizan el acceso de un usuario legítimo (ya sea robándolo del usuario legítimo o aprovechándose de la confianza de este).
2. **Agentes externos:** Este grupo hace referencia a los no usuarios del sistema. De esta forma se consigue acceso al recurso o servicio sin necesidad de ser un usuario legítimo (un sistema que no controle la autenticación de usuarios).

   En este grupo usualmente se falsea la dirección de origen (faked/spoofed IP) con el propósito de evitar el origen real del ataque. Además, cabe recalcar que gran parte de la peligrosidad de este tipo de ataques por red viene dada por su independencia de plataforma hardware o sistema operativo.

   Debido a que el protocolo IP permite una comunicación homogénea (independiente del tipo de ordenador o fabricante) a través de espacios heterogéneos (redes ETHERNET, ATM, etc), un ataque exitoso contra el protocolo IP se convierte inmediatamente en una amenaza real para todos los ordenadores conectados a Internet.

4.1.2 DETECCIÓN DE ATAQUES DoS

Pueden ocurrir una gran variedad de ataques DoS. Los ataques DoS mas comunes utilizan **UDP echos (fraggle), ICMP echo and replies (Smurf) y TCP (TCP SYN flooding).**

Sin embargo, nunca se debe asumir que los ataques DoS que se estan experimentando en la red fallan sobre cualquiera de estos tres tipos: Algunas fallas no suceden sobre estas tres categorias.

4.1.2.1 ATAQUES COMUNES

Entre los ataques DoS mas comunes se incluyen:

Smurf

Es un ataque DoS que usa solicitudes ICMP. El nombre de Smurf es usado porque este fue el nombre original que el hacker le dio a la aplicación.

En un ataque Smurf, el atacante envía una inundación de mensajes ICMP para un reflector o conjunto de reflectores. El hacker cambia estas direcciones a la dirección del dispositivo o dispositivos de la victima actual. Entonces los reflectores inocentemente contestan los mensajes echo, inadvertidamente envían las respuestas a la victima. En muchos casos, la dirección origen es una dirección de broadcast dirigida, permitiendo que el ataque apunte un segmento de la red en vez de un host especifico.

Un método para prevenir este ataque es utilizar el comando: **no ip directed-broadcast** en la interfaz del router.

El protocolo ICMP es el encargado de realizar el control de flujo de los datagramas IP que circulan por Internet. Este protocolo consta de diversas funcionalidades que permiten desde la comunicación de situaciónes anómalas (no se ha podido realizar la entrega del paquete IP) hasta la comprobación del estado de una máquina en Internet (ping - pong o ECHO - ECHO REPLY).

Este tipo de ataque se basa en falsear las direcciones de origen y destino de una petición ICMP de ECHO (ping).

Como dirección de origen se coloca la dirección IP de la máquina que va a ser atacada. En el campo de la dirección de destino se situa la dirección broadcast de la red local o red que se utilizara como “lanzadera” para colapsar al sistema elegido.
Con esta petición fraudulenta, se consigue que todas las máquinas de la red contesten a la vez a una misma máquina, consumiendo el ancho de banda disponible y saturando al ordenador elegido.

Fraggle Attack

Utiliza paquetes de solicitud UDP en la misma manera que se utilizan los paquetes de solicitud de ICMP; este ha sido una simple re-escritura de “Smurf”. Utiliza UDP.
Tanto en los ataques Smurf como en los Fraggle, hay tres partes en estos ataques: el atacante, el intermediario y la victima (hay que tomar en cuenta que el intermediario también puede ser una víctima. Es decir que, hay que tener precaución de ser afectado de una de las siguientes maneras:

Como una victima o blanco de el ataque.
Como red que se abusa para ampliar el ataque.
Como una parte de quién inicia el ataque.

TCP SYN flood Attacks

Es un ataque fácil de iniciar. El atacante envía un flujo de segmentos TCP SYN con la intención de no terminar la comunicación de tres vías “tree – way handshake” para cada una de las conexiones. Típicamente el hacker combina esto con un ataque spoofing IP en el que paquete en la dirección origen se invalida en la dirección de alguien más. Porque esta dirección no puede ser alcanzada (o si son direcciones de alguien más no son respondidas).

Esta situación genera que el servidor espere hasta que el tiempo que TCP maneja expire para la conexión, antes de remover la conexión de su tabla local de conexión. Esto ocasiona problemas porque utiliza recursos sobre el servidor TCP ocasionando con esto que se denieguen conexiones legítimas de TCP.

IP Flooding

El ataque de IP Flooding (inundación de paquetes IP) se realiza habitualmente en redes locales o en conexiones con un gran ancho de banda disponible.
Consiste en la generación de tráfico espurio con el objetivo de conseguir la degradación del servicio de red. De esta forma, el atacante consigue un gran consumo del ancho de banda disponible ralentizando las comunicaciones existentes en toda la red.
Se da principalmente en redes locales dónde el control de acceso al medio es nulo y cualquier máquina puede enviar/recibir sin ningún tipo de limitación en el ancho de banda consumido.
El tráfico generado en este tipo de ataque puede ser:
• Aleatorio: Cuando la dirección de origen o destino del paquete IP es ficticia o falsa. Este tipo de ataque es el más básico y simplemente busca degradar el servicio de comunicación del segmento de red dónde el ordenador responsable del ataque está conectado.
• Definido o dirigido: Cuando la dirección de origen, destino (o ambas) es la de la máquina que recibe el ataque. El objetivo de este ataque es doble, ya que además del colapso del servicio de red dónde el atacante genera los paquetes IP busca colapsar un ordenador destino, ya sea reduciendo el ancho de banda disponible para que siga ofreciendo el servicio o colapsar el servicio ante una gran cantidad de peticiones que el servidor será incapaz de procesar.

Este tipo de ataque por inundación se basa en la generación de datagramas IP de forma masiva. Estos datagramas pueden ser de los tipos siguientes:
• UDP: Generar peticiones sin conexión a cualquiera de los 65535 puertos disponibles. En muchos sistemas operativos, las peticiones masivas a puertos

específicos UDP (ECHO, WINS, etc) causan el colapso de los servicios que lo soportan.

• ICMP: Generación de mensajes de error o control de flujo malicioso. En este caso el objetivo es doble, degradar el servicio de red con la inundación de peticiones y / o conseguir que los sistemas receptores queden inutilizados por no poder procesar todas las peticiones que les llegan.

• TCP: Genera peticiones de conexión con el objetivo de saturar los recursos de red de la máquina atacada. Este protocolo es orientado a conexión, y como tal consume recursos de memoria y CPU por cada conexión. El objetivo es el de saturar los recursos de red disponibles de los ordenadores que reciben las peticiones de conexión y degradar la calidad del servicio.

Broadcast

En el protocolo IP también existe una forma de identificar la red a la que pertenece la dirección IP, para ello simplemente debemos sustituir los bits de la máscara de red por ceros. Análogamente, IP también tiene un sistema de radiodifusión (broadcast) que permite la comunicación simultánea con todos los ordenadores de la misma red. Para realizar esta operación simplemente debemos sustituir los bits de la máscara de red por unos.

En este tipo de ataque se utiliza la dirección de identificación de la red IP (broadcast address) como dirección de destino del paquete IP. De esta forma, el router se ve obligado a enviar el paquete a todos los ordenadores pertenecientes a la red, consumiendo ancho de banda y degradando el rendimiento del servicio.

También existen variantes dónde se envían peticiones de PING a varios ordenadores falseando la dirección IP de origen y substituyéndola por la dirección de broadcast de la red a atacar.

Este ataque al igual que el IP Flooding se suele realizar en redes locales ya que requiere un gran ancho de banda por parte del atacante, aunque con la mejora de las comunicaciones y anchos de banda disponibles es factible realizarlo remotamente.

PING OF DEATH

El PING de la muerte (Ping of death) ha sido probablemente el ataque de negación de servicio mas conocido y que mas artículos de prensa ha conseguido.
Este ataque utiliza una vez mas las definiciones de la longitud máxima de paquetes de los protocolos IP / UDP / TCP / ICMP así como la capacidad de fragmentación de los datagramas IP.
La longitud máxima de un datagrama IP es de 64K (65535 Bytes) incluyendo la cabecera del paquete (20 Bytes) y asumiendo que no hay opciónes especiales especificadas.
El protocolo ICMP es el que se utiliza para la comunicación de mensajes de control de flujo en las comunicaciones (si la red está congestionada, si la dirección de destino no existe o es inalcanzable) y tiene una cabecera de 8 bytes.
De esta forma se tiene que para enviar un mensaje ICMP se dispone de 65535 - 20 - 8 = 65507 Bytes.
En el caso de enviar más de 65535 bytes el paquete se fragmenta y se reconstruye en el destino utilizando un mecanismo de posición y desplazamiento relativo.
No obstante, si se envian ordenes al sistema operativo para que envíe un datagrama con una longitud de 65510 bytes (correcto, puesto que es inferior a 65507 bytes):
ping -l 65510 direcion_ip [Windows]
ping -s 65510 direccion_ip [Unix]
Se obtiene que el tamaño es inferior a los 65535 con lo que los datos a enviar cogen en un único paquete IP (fragmentado en N trozos, pero pertenecientes al mismo datagrama IP).
Sumando el tamaño de las cabeceras se obtiene:
20 bytes cabecera IP + 8 bytes cabecera ICMP + 65510 bytes de datos = 65538.
Sin embargo debido a la cabecera ICMP el espacio disponible tan sólo era de 65507 bytes. En consecuencia al reensamblar el paquete en el destino se suelen producir errores de overflow / coredump que causan la parada del servicio o del sistema atacado.

Ataques Distribuidos DoS (DDoS)

En un ataque distribuido DoS, los múltiples origenes son tráfico de inundacion, si es: ICMP, los segmentos de bandera de control TCP (tales como con SYN) o flujo de UDP. Este puede ser algo tan simple como un hacker enviando múltiples corrientes de broadcasts dirigido para diferentes subredes y que estas subredes tengan que responder con contestaciones a las solicitudes de la victima. Sin embargo, muchos ataques DDDoS son mucho mas sofisticados que los ataques simples de Smurf o de Fraggle.

El enfoque clásico utilizado en las herramientas de DDOS se basa en conseguir que un gran número de máquinas comprometidas (slaves) dirijan un ataque directo hacía un destino concreto.

El objetivo principal es el de concentrar el mayor número de máquinas bajo control puesto que mas máquinas significará mas potencia de ataque y por lo tanto mas consumo de ancho de banda de la víctima.

Si se tiene por objetivo, dejar fuera de funcionamiento los servidores atacados, si se degrada mucho la calidad del servicio de comunicaciones de red (aunque los servidores sigan funcionando) el ataque puede considerarse exitoso.
Este tipo de modelo tiene varios inconvenientes, entre ellos que se necesita obtener el control de todas las máquinas implicadas en el proceso (masters / slaves). Esto implica la obtención de un ataque exitoso para cada máquina bajo control y además que no se detecte la presencia por el administrador de red.

Se puede definir el ataque de denegación de servicio distribuido (DDOS) como un ataque de denegación de servicio (DOS) dónde existen múltiples focos distribuidos y sincronizados que focalizan su ataque en un mismo destino.

Otra opción consiste en usar técnicas de reflexión. La táctica simplemente consiste en enviar cientos de miles de peticiones a servidores con grandes conexiones a Internet (ISP por ejemplo) falseando la dirección de origen con el objetivo de que las respuestas inunden a la víctima.

Con este tipo de táctica, el atacante consigue un doble objetivo:
1. Se esconde el origen real de el ataque. Esto significa que el hecho de que se realice un ataque no pone de manifiesto inmediatamente las fuentes de este, lo que le permite seguir manteniendo un control de las máquinas. Cuando los servidores que reciben la reflexión corten el acceso se puede dirigir a otros servidores (hay cientos de grandes ISP en Internet) y continuar el ataque.
2. Se ahoga a la víctima durante un período de tiempo mayor. Si se va cambiando los ordenadores a los cuales se les realizan las peticiones, el bombardeo de peticiones continúa desde diferentes puntos de Internet, evitando cualquier posibilidad de defensa.

Los cinco principales ataques DDDoS:
Los hackers utilizan cinco tipos de ataques DDDoS principales para implementar sus ataques:

- Tribe Flood Network (TFN)
- Tribe Flood Network 2K (TFN2K)
- Trinoo
- Stacheldraht
- Trinity

TFN

Existen dos variedades de TFN: TFN y TFN2K. TFN es un programa DDDoS que fue desarrollado por un hacker aleman a mediados de 1999. Cuando se separan, los clientes son capaces de lanzar todo tipo de ataques DoS, incluyendo ICMP, inundaciones UDP, inundaciones TCP SYN y ataques Smurf. Despues que TFN esta instalado, el hacker puede usar una variedad de métodos de conexiones para controlar los clientes, incluyendo Telnet. La comunicación entre los dispositivos se compromete con mensajes de solicitud ICMP.

Porque los mensajes de respuesta a las solicitudes ICMP son el corazón del sistema de comunicación TFN, la detección de este ataque es difícil. La mejor manera de bloquear TFN es restringir el flujo de paquetes de respuesta a las solicitudes de ICMP.

TFN2K

Es una extensión de TFN. Contrario a TFN, TFN2K usa paquetes UDP, ICMP y TCP para comunicarse; con TCP y UDP, los números de puertos son al azar. Para hacerlo menos perceptible, dos o tres de estos protocolos IP pueden ser usados. Además, TFN2K utiliza un cifrado mucho mas fuerte para proteger los mensajes y datos de el agente. Porque este usa paquetes TCP, UDP e ICMP, que pueden ser seleccionados al azar y también cifrar los mensajes, es imposible filtrar este tráfico con un Firewall de filtro de paquetes normal, tal como las listas de control de acceso extendidas de la IOS Cisco.

Trinoo

Fue descubierto en Agosto de 1999. Un hacker útilizo mas de 100 sistemas comprometidos para implementar un ataque DddoS a partir de 227 amplificadores, bajando un servidor critico de la Universidad de Washington por dos dias. La especulación tambien presento que Trinooo fue usado para traer abajo a Yahoo y otros principales sitios de Internet con una inundación de paquetes UDP. Para instalar el cliente, el hacker uso una hazaña del sobrante del almacenador

intermediario para tener acceso no autorizado a los agentes. En un punto, mas de miles de agentes fueron sospechosos por iniciar el compromiso. Después de comprometer el sistema, el hacker instalo un daemon por medio del cual puede controlar remotamente con un programa principal (tipicamente atraves de Telnet) para enviar sus instrucciones a su tropa de agentes. Sus instrucciones son tipicamente simples: se especifica el destino de el ataque y por cuanto tiempo ocurre el ataque.

STACHELDRAHT *(del alemán alambre de espinas)*

Es una herramienta de ataques DDOS basada en código del TFN que añade algunas características más sofisticadas como el cifrado en el intercambio de mensajes.
Como en TRINOO, la arquitectura básica de STACHELDRAHT mantiene una jerarquía dónde existen los master (denominados ahora “handlers”, manipuladores o controladores) y demonios/daemons o bcast (denominados ahora “agents” o agentes).Los ataques permitidos en STACHELDRAHT al igual que en el TFN son ICMP Flood, UDP Flood, SYN Flood y SMURF.
Stacheldraht tambien soporta actualizaciónes automáticas de el programa daemon, permitiendo que el hacker modifique el código que ha usado, para hacerlo menos susceptible a la detección.
Cada amo puede controlar hasta 1000 agentes instalados de modo insospechado, el ataque de un hacker inicia con una frase de intrusión masiva, en el cual muchas computadoras son atacadas y el hacker obtiene un acceso no autorizado. El programa de daemon del agente es instalado y espera por un comando para implementar un ataque DDDoS contra una victima.

TRINITY

Es uno de los más nuevos ataques DDDoS descubierto. Trinity es mucho más ingenioso en el método de compartir comandos entre el master y el agente. Primero el hacker obtiene acceso no autorizado a un sistema UNIX e instala el programa /usr/lib/idle.so. Cuando se activa, este programa se conecta a un servidor IRC en el

puerto 6667. Entonces el cliente envia su nickname del IRC a las primeras tres letras del nombre de la victima, seguido por tres letras al azar. Por ejemplo, el nombre de la víctima es www.quizware.com, el nickname podria ser algo tal como quiabc. Despues de enviar el nickname, el cliente ensambla el canal #b3ebl3br0x, usando una llave especial. Entonces el cliente espera pacientemente instrucciones.

4.1.2.2 DEFENSAS CONTRA DOS/DDOS

PREVENCIÓN DE ATAQUES

Fraggle es muy similar a Smurf, pero Fraggle usa UDP **echos** en lugar de ICMP **echos-basically,** alguien recodifico Smurf para trabajar con UDP. Dando el impacto enorme que juntos estos dos programas tiene.

Pueden realizarse cinco cosas basicas para limitar que este tipo de ataques afecten a la red:

- Apagar las redes con los amplificadores.
- Deshabilitar las direcciones de broadcast dirigidas.
- Realizar el filtro para ingreso y egreso de direcciones de broadcast dirigidas.
- Implementar Rate Limiting atraves de CAR. Esto no previene el ataque, pero limita la cantidad de ancho de banda que las solicitudes de ICMP y UDP (o respuestas) pueden usar.
- Utilizar la verificación de Reverse-Path-Forwarding para IP unicast con la finalidad de prevenir IP spoofing.
- El límite de velocidad mediante mecanismos, tal como la velocidad de acceso comprometida (CAR), controla el tráfico en ambos puntos de ingreso y de egreso de la red del proveedor de servicios, de este modo, reduciendo los ataques DOS y DOS distribuidos (DDoS).
- Filtrar paquetes que contienen una dirección origen de una red diferente por que el ataque Smurf confía en el uso de paquetes forjados.
- Apagar el reenvío de broadcasts dirigidos en los puertos del Router o tomar otras medidas para asegurarse que la red no pueda ser abusada en este modo.

4.1.3 ATAQUES DE AUTENTICACIÓN

Este tipo de ataque tiene como objetivo engañar al sistema de la víctima para ingresar al mismo. Generalmente este engaño se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y password.

Spoofing-Looping

Spoofing puede traducirse como "hacerse pasar por otro" y el objetivo de esta técnica, justamente, es actuar en nombre de otros usuarios, usualmente para realizar tareas de Spoofing.

Una forma común de Spoofing es conseguir el nombre y password de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él.

El intruso usualmente utiliza un sistema para obtener información e ingresar en otro, y luego utiliza este para entrar en otro, y así sucesivamente. Este proceso, llamado Looping, y tiene la finalidad de "evaporar" la identificación y la ubicación del atacante.

El envío de falsos e-mails es otra forma de Spoofing que las redes permiten. Aquí el atacante envía E-Mails a nombre de otra persona con cualquier motivo y objetivo.

Tal fue el caso de una universidad en EE.UU. que en 1998, que debió reprogramar una fecha completa de exámenes ya que alguien en nombre de la secretaría había cancelado la fecha verdadera y enviado el mensaje a toda la nómina de estudiantes.
Muchos ataques de este tipo comienzan con Ingeniería Social y los usuarios, por falta de cultura, facilitan a extraños sus identificaciones dentro del sistema usualmente través de una simple llamada telefónica.

Spoofing

Este tipo de ataques (sobre protolocos) suele implicar un buen conocimiento del protocolo en el que se va a basar el ataque. Los ataques tipo Spoofing bastante conocidos son el: IP Spoofing, el DNS Spoofing y el Web Spoofing IP Spoofing.

Con el IP Spoofing, el atacante genera paquetes de Internet con una dirección de red falsa en el campo From, pero que es aceptada por el destinatario del paquete. Su utilización más común es enviar los paquetes con la dirección de un tercero, de forma que la víctima "ve" un ataque proveniente de esa tercera red, y no la dirección real del intruso.
Este ataque se hizo famoso al usarlo Kevin Mitnick.

DNS Spoofing

Este ataque se consigue mediante la manipulación de paquetes UDP pudiéndose comprometer el servidor de nombres de dominios (Domain Name Server-DNS) de Windows NT(c). Si se permite el método de recursión en la resolución de "Nombre"Dirección IP" en el DNS, es posible controlar algunos aspectos del DNS remoto. La recursión consiste en la capacidad de un servidor de nombres para resolver una petición de dirección IP a partir de un nombre que no figura en su base de datos. Este es el método típico (y por defecto) de funcionamiento.

Web Spoofing

En el caso Web Spoofing el atacante crea un sitio web completo (falso) similar al que la víctima desea entrar. Los accesos a este sitio están dirigidos por el atacante, permitiéndole monitorizar todas las acciones de la víctima, desde sus
datos hasta las passwords, números de tarjeta de créditos, etc. El atacante también es libre de modificar cualquier dato que se esté transmitiendo entre el servidor original y la víctima o viceversa.

IP Splicing-Hijacking

Se produce cuando un atacante consigue interceptar una sesión ya establecida. El atacante espera a que la víctima se identifique ante el sistema y tras ello le suplanta como usuario autorizado.

Utilización de BackDoors

"Las puertas traseras son trozos de código en un programa que permiten a quien las conoce saltarse los métodos usuales de autentificación para realizar ciertas tareas. Habitualmente son insertados por los programadores del sistema para agilizar la tarea de probar código durante la fase de desarrollo".

Esta situación se convierte en una falla de seguridad si se mantiene, involuntaria o intencionalmente, una vez terminado el producto ya que cualquiera que conozca el agujero o lo encuentre en su código podrá saltarse los mecanismos de control normales.

Utilización de Exploits

Es muy frecuente ingresar a un sistema explotando agujeros en los algoritmos de encriptación utilizados, en la administración de las claves por parte la empresa, o simplemente encontrado un error en los programas utilizados.
Los programas para explotar estos "agujeros" reciben el nombre de Exploits y lo que realizan es aprovechar la debilidad, fallo o error hallado en el sistema (hardware o software) para ingresar al mismo. Nuevos Exploits (explotando

nuevos errores en los sistemas) se publican cada día por lo que mantenerse informado de los mismos y de las herramientas para combatirlos es de vital importancia.

Obtención de Passwords

Este método comprende la obtención por "Fuerza Bruta" de aquellas claves que permiten ingresar a los sistemas, aplicaciones, cuentas, etc. atacados. Muchas passwords de acceso son obtenidas fácilmente porque involucran el nombre u otro dato familiar del usuario y, además, esta nunca (o rara vez) se cambia. En esta caso el ataque se simplifica e involucra algún tiempo de prueba y error. Otras veces se realizan ataques sistemáticos (incluso con varias computadoras a la vez) con la ayuda de programas especiales y "diccionarios" que prueban millones de posibles claves hasta encontrar la password correcta.

Uso de Diccionarios

Los Diccionarios son archivos con millones de palabras, las cuales pueden ser passwords utilizadas por los usuarios. Este archivo es utilizado para descubrir dicha password en pruebas de fuerza bruta. El programa encargado de probar cada una de las palabras encripta cada una de ellas (mediante el algoritmo utilizado por el sistema atacado) y compara la palabra encriptada contra el archivo de passwords del sistema atacado (previamente obtenido). Si coinciden se ha encontrado la clave de acceso al sistema mediante el usuario correspondiente a la clave hallada.

Actualmente es posible encontrar diccionarios de gran tamaño orientados, incluso, a un área específico de acuerdo al tipo de organización que se esté atacando.

La velocidad de búsqueda se supone en 100.000 passwords por segundo (este número suele ser mucho mayor dependiendo del programa utilizado). Aquí puede observarse la importancia de la utilización de passwords con 8 caracteres de longitud (al menos) y con todos los caracteres disponibles.

4.1.4 ROUTING PROTOCOLS **[3]**

Los protocolos de enrutamiento pueden ser vulnerados principalmente mediante la introducción de paquetes de actualización de rutas, de forma que es posible adecuar y condicionar los caminos que seguira el tráfico según un criterio específico.

Uno de los protocolos que puede ser falseado (spoofing) es RIP [RP-1], en su versión 1, RFC 1058 y 2, RFC 1723. Se trata de un protocolo UDP (puerto 520), por tanto acepta paquetes de cualquier sistema sin necesitar ninguna conexión previa. La versión 1 no dispone de sistema de autenticación, mientras que la versión 2 presenta un método basado en el envío de claves en claro de 16 bytes.

Para vulnerar RIP, como se especifica a continuación, es necesario inicialmente identificar un *router* que hable este protocolo a través de la identificación del puerto UDP 520. En el caso de pertenecer al mismo segmento de red, deben escucharse las actualizaciónes RIP que circulan por la red o solicitarselas directamente a alguno de los *routers.* De esta forma se obtendrá la tabla de rutas que se anuncia en ese momento. Si no se esta en el mismo segmento, se dispone de herramientas como **rprobe** para realizar una peticion RIP remota: el resultado se obtendra mediante un *sniffer* en el sistema desde el que se ataca.

Una vez definida la información que se pretende inyectar en la tabla de rutas anunciada, por ejemplo, redireccionar todo el tráfico a un sistema desde el que se pueda analizar el mismo, meidante útilidades como *scrip,* se inyectará la ruta deseada. A partir de ese momento todo el flujo de tráfico pasará por el nuevo camino definido. Para que el funcionamiento habitual no se vea modificado, es necesario que el nuevo sistema al que van destinado los paquetes los redireccione consecuentemente: *ip forwarding.*

SOURCE ROUTING

Esta funcionalidad propia del protocolo IP permite enviar dentro del mismo paquete de datos la información necesaria para su enrutamiento, es decir, la dirección IP de cada uno de los dispositivos de red intermedios que deben cruzarse hasta llegar al destino final.

Esta caracteristica puede emplearse para tareas de verificación y configuración de los enlaces, pero desde el punto de vista de la seguridad supone que un atacante es capaz de manejar por donde deben viajar sus paquetes IP, saltandose todas las reglas de enrutamiento definidas en los dispositivos de red. Asimismo, puede permitir la realización de pruebas para conocer las redes internas y tambien permitir a un atacante el alcanzar redes con IP's internas (RFC 1918).

Unida a la técnica de *IP spoofing* permite que un atacante se haga pasar por otro sistema IP, siendo capaz de enviar y recibir todas las respuestas asociadas a una comunicación falseada.

ROUTING PROTOCOLS

Los protocolos de enrutamiento pueden protegerse garantizando la autenticación del sistema de red que envia la actualización de la tabla de rutas asi como encriptando los datos, con el objetivo de prevenir la insercion de actualizaciónes falsas.

Los protocolos BGP, IS-IS y OSPF contemplan la posibilidad de autenticación e integridad en base al algoritmo de *hashing* MD5. El método empleado se basa en el conocimiento mutuo de una clave entre los dispositivos que intercambian rutas, enviandose cada actualización acompañada de un *fingerprint* o firma, obteniendo a partir de la clave y el propio contenido de la actualización.

Se recomienda deshabilitar los paquetes RIP de entrada en los *routers* externos, pudiendo emplear el protocolo internamente en la red.

4.2 IMPLEMENTACIÓN DE TÉCNICAS DE FILTRADO

4.2.1 LISTAS DE CONTROL DE ACCESO (ACL) **[4]**

Las listas de acceso también llamadas listas de control de acceso (ACL, Access Control List), constituyen los mecanismos principales de filtrado de paquete en la mayor parte de los Routers de Cisco. Asi mismo, las ACL, se utilizan para otra serie de funciones, incluyendo el filtrado de ruta y la utilización de determinados comandos show. Por ello, resulta necesario tener un sólido conocimiento sobre las ACL, para poder resolver cualquier clase de problema y configurar los equipos de Cisco en la mayoría de las redes. Las ACL, permiten controlar que clase de coincidencia efectúa un Router en relación con una determinada función, como el envió de paquetes.

Por ejemplo, si no existe una forma de especificar de forma condicional que paquetes pueden enviarse de una red a otra (como es el caso de Internet), el usuario tendrá que autorizar el envio de todos los paquetes (lo cual hace que la red en cuestión sea un objetivo sencillo para los hackers), o bien denegar todos los paquetes (lo que haría imposible la conectividad). El control general a través de filtrado de paquete constituye una función primaria de las ACL. Sin embargo, las ACL se pueden utilizar con comandos más complejos (como los mapas de ruta o las listas de distribución), lo que proporciona un grado de control muy preciso sobre la funcionalidad del enrutador.

Los objetivos básicos del filtrado de paquete resultan muy sencillos. Consiste en acceder exclusivamente a recursos específicos situados en una red privada desde una red remota (generalmente, una red pública como Internet).

4.2.1.1 COMPRENDER EL FILTRADO DE PAQUETE

Los objetivos básicos del filtrado de paquete resultan muy sencillos. Supongamos que se desea que una red remota (generalmente, una red pública como Internet) acceda exclusivamente a recursos específicos situados en una red privada, al tiempo que se autoriza el acceso de la red privada a la red remota. La red interna es la red que se desea proteger de un acceso realizado desde el exterior.

Finalmente, cuando se trabaja con filtros es preciso comprender el concepto de *dirección* (o sentido del flujo): el tipo de tráfico, entrante o saliente, al que se aplica el filtro.

Si la dirección es *entrante,* el filtro se aplica al tráfico introduciendo la interfaz desde la red vinculada. En el caso de una interfaz interna, el tráfico entrante no es otra cosa que el tráfico que introduce la interfaz desde la red interna. Si este tráfico se enruta hacia la red externa, tendría que considerarse tráfico saliente en la interfaz externa. Si la dirección es *saliente,* el filtro se aplica al tráfico que abandona la interfaz en la red vinculada. En el caso de una interfaz interna se trata de tráfico enviado desde la interfaz interna a la red interna. Si este tráfico se enruta desde la red externa, también se debe considerar tráfico entrante en la interfaz externa.

(Ver demostración de configuración de técnica en cd-anexo: video #7: NAT, video #11: VPN, video #12: Failover, video #13: AP, video #14: NBAR, video #15: Url Filtering, la configuración de ACL es demostrada en estas técnicas)

4.2.2 FILTRADO DE URL[3]

El filtrado de URL es una opción muy útil a la hora de administrar la red, para bloquear sitios web problemáticos (o definidos por la organización) como sitios web no permitidos.
Ya que puede utilizarse el filtrado de URL para bloquear sitios Web, servidores de descarga y servicios de correo electrónico HTTP personales.

Así como la IOS 12.2(11)YU la IOS 12.2(15)T de Cisco, soportan filtrado de URL. Uno de los problemas de hacer uso de ACL extendidas o Inspección mediante CBAC con el bloqueo de Java es que el Router filtra solo el tráfico que se ha definido en las ACL o en la declaración de Inspección. Como ejemplo imágenes pornográficas que se desean prevenir, juegos, archivos compartidos, se podría realizar mediante ACL extendidas, sin embargo se tendría que conocer cada dirección IP de las computadoras.
Desafortunadamente, no se puede defender de cada pagina Web, si se necesita bloquear cada una de estas páginas de estos servidores se tendrían fácilmente millares de entradas del ACL que mantener.

Debido a estos inconvenientes, típicamente las ACLs no se utilizan para implementar esta clase de políticas de seguridad. En lugar, se utiliza un servidor de contenido-filtrado. Cisco apoya actualmente productos del servidor de N2H2 (Sentian) y de Websense para realizar este procedimiento de filtrado. Realmente, los servidores de contenido-filtración contienen las políticas del acceso, y el Router de Cisco utiliza estas políticas externas para hacer cumplir el acceso de URL de sus usuarios.

A continuación se muestran los parámetros de sugerencia para implementar filtrado de URL utilizando Router Cisco y un servidor externo de N2H2 o de Websense.

4.2.2.1 VENTAJAS Y LIMITACIONES DE USAR FILTRADO DE URLS

4.2.2.1.1 VENTAJAS DE USAR FILTRADO DE URL

El filtrado del URL proporciona muchas ventajas y ofrece una solución robusta de la seguridad para su red, incluyendo las ventajas siguientes:

- Con un servidor de filtrado de contenido, se hace más fácil poder implementar las políticas basadas en tipos de acceso, tales como deportes, pornografía, juego, política, ocio, religión, y otras agrupaciones de información. Sin embargo, todavía se pueden definir reglas propias y restricciones de acceso basadas en hosts o usuarios.

- Las actualizaciónes automáticas pueden ser descargadas en servidor de contenido para los sitios nuevos que pertenecen a las categorías especificadas, así como remover links muertos que ya no funcionan. Esto reduce mucho los gastos indirectos de gerencia de tener que hacer este proceso manualmente.

- Se puede guardar un detallado de los accesos en el Websense o N2H2 del servidor de contenido de quién está teniendo acceso a qué recursos. Esto es importante para la responsabilidad cuando llega la hora de identificar quienes irrespetan las reglas y desarrollar estadísticas sobre el tipo de acceso que tienen los usuarios.

- Pueden definirse políticas basadas en host o por usuario, proporcionando más control sobre las políticas de acceso.

- Se puede definir múltiples servidores para filtrado de contenido en el router lo cual provee redundancia. En esta situación, uno de los servidores de filtrado de contenido es definido como primario y el router envia todo el tráfico a este. Si el servidor primario no es accesible o esta bajo, el router puede usar un servidor secundario configurado. Si todos los servidores estan abajo, se tiene la opción de no permitir o prevenir todo el tráfico http al router.

- La IOS Cisco puede proteger hasta 200 peticiones HTTP simultáneas, para reducir la probabilidad de que conexiones http caigan debido a inconvenientes en el tiempo de respuesta entre el router y el servidor de filtrado de contenido

4.2.2.1.2 RESTRICCIONES DE FILTRADO DE URLS

A continuación se presentan restricciones de filtrado de URL sobre N2H2 y de Websense. Se recomienda utilizar solamente un producto: La IOS de Cisco no soporta ambos productos simultáneamente. N2H2 y Websense tienen las restricciones siguientes:

- Se puede especificar múltiples servidores de N2H2 o de Websense para la redundancia. Sin embargo, el IOS del Cisco utiliza activamente solamente un servidor.

- La disposición de filtrado de URL trabaja unicamente con un producto de filtrado de contenido: Websense o N2H2. Cisco no soporta el uso de ambos productos simultáneamente en los router.

- Solamente el protocolo TCP es soportado para la conexión entre el router y el servidor N2H2 (Websense soporta TCP y UDP).

(Ver demostración de configuración de técnica en cd-anexo: video #15: Url Filtering)

4.3 CONTROL DE ACCESO BASADO EN CONTEXTO (CBAC) [3]

Lleva un registro de las conexiones que se están supervisando, además construye una tabla de estado similar a la que crea los Cisco PIX; además supervisa TCP, UDP y conexiones ICMP. CBAC usa la tabla de estado para crear listas de accesos dinámicas con el fin de permitir devolver el tráfico a través del perímetro de red.

4.3.1 FUNCIONES DE CBAC

Provee 4 funciones principales:

- Filtrado de Tráfico
- Inspección de Tráfico
- Detección de Intrusos
- Generación de Alarmas

a) Filtrado de Tráfico: Una de las funciones principales de CBAC es filtrar tráfico, específicamente para las conexiones TCP, UDP e ICMP. Al igual que las ACLs Reflexivas permite retornar tráfico en la red interna; sin embargo también puede ser utilizada para filtrar el tráfico que se origina en cualquiera de los lados, ya sea red interna o externa.
CBAC soporta inspección de aplicación, significando esto que puede examinar el contenido de cierto tipo de paquetes cuando realiza el proceso de filtrado. Por ejemplo, puede examinar comandos SMTP en una conexión SMTP. También puede examinar los mensajes de una conexión para determinar el estado de una conexión. Por ejemplo, FTP hace uso de dos conexiones, una de control y otra de conexión de datos. CBAC puede examinar la conexión de control, determinando con ello que se está estableciendo una conexión de datos y agregar a esta conexión una tabla de estado. CBAC puede examinar conexiones http para los Java Applets y filtrarlos si así se desea.

b) Inspección de Tráfico: CBAC puede examinar información de la capa de aplicación y utilizar esto para mantener el registro de conexiones del Firewall, incluso para las aplicaciones que abren múltiples conexiones o se conectan a la dirección NAT.

   Este proceso de la inspección permite no solo devolver nuevamente el tráfico dentro de la red, sino que también puede ser utilizado para prevenir de ataques de Inundación TCP. CABAC puede examinar la tarifa asignada de cada conexión y puede cerrar estas conexiones si se alcanza un nivel especificado. También puede examinar conexiones TCP y botar cualquier paquete sospechoso. Además examinando conexiones TCP puede examinar tráfico proveniente de Ataques DoS.

c) Detección de Intrusos: CBAB puede proporcionar protección contra los ataques de Correo, limitando el tipo de comandos SMTP que pueden ser enviados a los Servidores de Correo Internos. Ante estos tipos de ataques, CBAC puede generar información acerca del ataque y de manera opciónal el poder reiniciar la conexiones TCP para interrumpir el flujo de paquetes sospechosos.

d) Generación de Alarmas: CBAC puede generar alarmas en tiempo real de los ataques detectados, así como proporcionar un rastro detallado de la conexión solicitada. Por ejemplo: se puede registrar todas las peticiones de conexión de red, incluyendo las direcciones IP fuente y destino, los puertos utilizados en dicha conexión y el número de octetos enviados, el tiempo de inicio y finalización de la conexión.

Una de las características de CBAC es su flexibilidad en la configuración, ya que permite definir en cuál de las direcciones examinará el tráfico. El caso típico es utilizar CBAC en el perímetro Router/Firewall para permitir retornar el tráfico a la red. Sin embargo puede configurar CBAC para examinar tráfico en dos direcciones, tanto hacia fuera de la red como hacia dentro.

4.3.2 PROTOCOLOS SOPORTADOS POR CBAC

CBAC puede realizar la inspección en muchos protocolos, sin embargo la profundidad de su inspección no necesariamente será igual para cada protocolo. Los protocolos que soporta CBAC son los siguientes:

- Todas las sesiones TCP y UDP, incluyendo FTP, HTTP con Java, SMTP, TFTP y los comandos UNIX R tales como rexec, rlogin y rsh.
- Sesiones ICMP, incluyendo echo request, echo reply, destino inalcanzable, tiempo excedido, etc.
- RPCs (Sun Remote Procedure Calls)
- Oracle SQL*NET
- Aplicaciones H.323 y V2, incluyendo White Pine CU-SeeMe, Netmeeting y Proshare
- Real Time Streaming Protocol (RSTP definido en RFC 2326 y define cómo las secuencias de datos en tiempo real, voz y video se intercambian entre dispositivos), incluyendo aplicaciones como RealNetworks RealAudio G2 Player, Cisco IP/TV y Apple QuickTime.
- Protocolos de Voz sobre IP (VoIP), incluyendo el protocolo SCCP(Skinny Client Control Protocol; es un protocolo propietario de Cisco el cual fue diseñado para dar soporte y conectividad a teléfonos Cisco VoIP) y SIP (Session Initiation Protocol, es un protocolo estándar que define la interacción entre teléfonos VoIP, el cual está especificado en RFC 2327).

4.3.3 FUNCIONAMIENTO DE CBAC

Dadas todas las características de inspección de CBAC, esto puede poner una carga grande en el router, especialmente si se tratara de una red grande, la cual tenga sesiones simultáneas, las cuales deban ser inspeccionadas por CBAC. Por casa sesión que deba ser supervisada, se requieren 600 bytes de memoria. Si el router debe tratar con miles de conexiones, los requisitos de memoria deben ser altos, de igual manera la cantidad de procesamiento por parte del UCP.

CBAC proporciona tres características para el funcionamiento, ayudando a reducir la carga en el Router con función de Firewall:

- Mejora del rendimiento en cuanto a procesamiento.
- Mejora en conexiones por segundo.
- Mejora en la utilización del UCP.

4.3.4 LIMITACIONES DE CBAC

Incluso con todas las características y realces, CBAC no es la última solución para implementarse en un Firewall. CBAC tiene limitantes y no puede proteger contra todas las clases de ataques.

A continuación, algunas limitaciones de CBAC:

- Examina únicamente el tráfico especificado. Ésta es una ventaja y desventaja ya que permite tener el control de carga en el Router.
- CBAC no es simple de comprender y de poner en funcionamiento, ya que requiere del conocimiento detallado de protocolos y aplicaciones; así como también de su operación.
- La IOS de Cisco no puede usar CBAC para examinar el tráfico que el mismo Router origina.
- CBAC no examina los paquetes enviados al Router por sí mismo. El tráfico debe fluir a partir de otra interfaz para que la inspección ocurra.
- CBAC no puede examinar los paquetes cifrados, tales como IPSec. Sin embargo si la conexión VPN termina en el Router, puede examinar el tráfico que entra y sale del túnel VPN.
- CBAC no puede examinar transferencias de tres vías del FTP. Puede examinar solamente transferencias de dos vías pasivas o estándares.
- CBAC no soporta examinar todas las aplicaciones. Para ciertas aplicaciones, se necesita deshabilitar la inspección para que éstas funcionen correctamente.

4.3.5 CONFIGURACIÓN DE CBAC

El proceso de configuración se divide en 7 pasos:

1. Determinar que interfases serán internas y externas en el Router.
2. Crear ACLs para filtrar el tráfico entrante y cerciorarse de permitir el tráfico que deber ser examinado.
3. Cambie los valores de “timeout” para las conexiones. (Opciónal)
4. Configure PAM (Port Application Map) que especifica los números de puertos que CBAC debe examinar, si la aplicación está utilizando un número diferente al asignado por defecto, tal sería el caso que HTTP útilice el valor 8080. Este paso es opciónal ya que se requiere solamente en los casos que los números de puertos no sean los convencionales.
5. Defina las reglas de Inspección. Estas reglas definen que entradas se agregan a la tabla de estado y que tráfico es permitido. Si el tráfico es de salida no aplica la inspección.
6. Active la regla o reglas de la inspección en las interfaces del Router. El Router entonces utilizará CBAC para examinar el tráfico.
7. Probar la configuración enviando tráfico a través del Router con CBAC.

4.3.6 USO DE CBAC PARA PREVENCIÓN Y DETECCIÓN DE ATAQUES DOS

CBAC puede detectar ciertos tipos de ataques DoS. Cuando el ataque ocurre puede tomar cualquiera de las acciones siguientes:

- Bloqueo de paquetes
- Proteja el recurso interno de la red ante sobrecarga de las conexiones falsas.
- Genere un mensaje de alerta.

Para detectar ataques DoS, CBAC hace uso de valores de “timeout” y “threshold” para examinar las conexiones TCP. Cuando se establecen las conexiones TCP, generalmente no toman más que un segundo o dos. Además si las conexiones no se finalizan dentro de un período específico (30 segundos por defecto) , la IOS Cisco puede quitar esta información de la tabla de estado y notificar tanto el origen como el destino con un mensaje TCP RST. Esto se utiliza especialmente para mejorar el recurso interno ya que permite liberar las conexiones medio abiertas. Se pueden definir tres diversos umbrales para limitar el número de conexiones medio abiertas:

- Número total de sesiones medio abiertas TCP o sesiones incompletas UDP.
- Número total de sesiones medio abiertas TCP o sesiones incompletas en un período de tiempo determinado.
- Número total de sesiones medio abiertas TCP pos host.

Cuando se alcanzan estos niveles, la IOS Cisco puede comenzar a botar las conexiones incompletas que no se hayan eliminado, genera una alarma y/o bloquea el tráfico del dispositivo(s).

(Ver demostración de configuración de técnica en cd-anexo: video #16: CBAC)

4.4 NBAR (NETWORK BASED APPLICATION RECOGNITION) [3]

NBAR normalmente usado para implementar funciones de Calidad de Servicio, mejor conocidas como QoS (Quality of Service), en el Router. Se asegura que las aplicaciones reciban el ancho de banda necesario para funcionar correctamente.
Los parámetros que NBAR puede usar cuando configura QoS en una conexión incluyen ancho de banda, tiempo de retardo, variación en el retardo y paquetes perdidos, esto se logra identificando las aplicaciones o conexiones y asociándolas a una clase. La IOS Cisco utiliza esto para implementar QoS.

4.4.1 COMPONENTES DE QOS

QoS incluye los siguientes componentes:

- Clasificación. La clasificación se utiliza para separar diversas clases de tráfico en grupos distintos.
- Sello – Marca
- Administración del Congestionamiento.
- Evitación de la congestión.
- Mecanismos de Eficacia.
- Políticas.

4.4.2 NBAR Y SU CLASIFICACIÓN

La clasificación es el primer paso a implementar en el tema de Calidad de Servicio. NBAR sería como un motor de clasificación, el cual examina los paquetes y los clasifica basándose en el tipo de aplicación. Esto puede ser algo tan simple como examinar el número de puertos TCP o UDP en la cabecera de transporte de un segmento; o puede ser algo complejo como examinar información en cabeceras HTML. Básicamente NBAR puede examinar tráfico entre las Capas 3 y 7. Esta inspección puede buscar los siguientes tipos de información:

- Número de puertos TCP y UDP en los encabezados de segmentos de la capa de transporte.

- Asignación dinámica de número de puertos TCP y UDP para aplicaciones que requieran conexiones adicionales.
- Protocolos IP de capa 3.

La clasificación de tráfico con NBAR puede hacerse manualmente o dinámicamente. NBAR puede descubrir automáticamente protocolos de aplicación, esta característica mantiene estadísticas por protocolo tales como el número de paquetes entrantes y salientes. Con la clasificación manual se puede definir el tipo de tráfico que NBAR debería examinar.

4.4.3 NBAR Y FILTRADO DE TRÁFICO

NBAR normalmente es utilizado para implementar políticas de Calidad de Servicio; sin embargo puede ser adaptado fácilmente para aspectos de políticas de seguridad. Para ello se pueden hacer cumplir tres acciones básicas con NBAR:

- Filtrado de Tráfico: con esta política de filtrado, NBAR utiliza ACL para botar tráfico en la interfaz de salida. Esto requiere del uso de ACL extendidas.
- Tráfico Redirigido: con esta política de ruteo, NBAR hace uso de mapas de ruteo para determinar cómo el tráfico debería ser dirigido.
- Acciones de Registro: Permite llevar un registro de la acción de filtrado.

4.4.4 RESTRICCIONES DE NBAR

- El router no puede examinar tráfico si el Router es le origen o el destino del tráfico.
- El Router no puede examinar información en los fragmentos siguientes de un paquete; solo puede examinar el primer fragmento del paquete.
- Puede examinar solamente los primeros 400 bytes de un paquete.
- No soporta examinar continuas peticiones HTTP.
- No puede examinar tráfico encriptado, como HTTPS o IPSec.

Un detalle importante es que NBAR requiere aproximadamente 150 bytes de memoria RAM para examinar cada conexión. Para simplificar el proceso cuando se activa NBAR automáticamente se asignan 1 MB de memoria RAM. Si se da el caso de que se necesite más memoria, la IOS de Cisco automáticamente asigna de manera dinámica la memoria que se necesite. Cuando se decide hacer uso de NBAR primero se debe determinar el número de conexiones que el Router soporta para ser examinadas.

4.4.5 CONFIGURACIÓN BÁSICA DE NBAR

1. Activar CEF (Cisco Express Forwarding el cual permite el envío distribuido o balanceo de carga en cuanto a envío de paquetes se refiere).
2. Especificar los puertos No-estándares.
3. Clasificar el tráfico.
4. Descargar e instalar PDLMs (Packets Description Language Modules o Módulos de descripción de Paquetes). Esta es opcional.
5. Definir Políticas de tráfico
6. Activar la Política de tráfico en una interfaz.
7. Filtrar el tráfico marcado en la interfaz contraria.

(Ver demostración de configuración de técnica en cd-anexo: video #14: NBAR)

4.5 SISTEMAS DE DETECCIÓN DE INTRUSOS (IDS) [3]

4.5.1 ¿QUÉ ES UN SISTEMA DE DETECCIÓN DE INTRUSOS?

Un Sistema de Detección de Intrusos o IDS (Intrusión Detection System) es una herramienta de seguridad encargada de monitorizar los eventos que ocurren en un sistema informático en busca de intentos de intrusión.
Se define intento de intrusión como cualquier intento de comprometer la confidencialidad, integridad, disponibilidad o evitar los mecanismos de seguridad de una computadora o red. Las intrusiones se pueden producir de varias formas: atacantes que acceden a los sistemas desde Internet, usuarios autorizados del sistema que intentan ganar privilegios adicionales para los cuales no están autorizados y usuarios autorizados que hacen un mal uso de los privilegios que se les han asignado.

La detección de intrusos es la ciencia o en algunos casos el arte de detectar ataques a la redes. Las amenazas de seguridad se discuten en las siguientes 3 categorías básicas:

- Reconociendo los ataques
- Ataques de Denegación de servicios (DOS)
- Acceso de Ataques

IDS soluciones buscan detectar y algunas veces frustrar estas tres categorías de ataques.

4.5.2 IMPLEMENTACIÓN DE IDS

Para detectar y prevenir los ataques, las soluciones de los IDS son implementadas por uno de los dos métodos: perfiles o características o firmas.

PERFILES

Los sistemas de bases de perfiles se encarga de detectar la anomalías en el tráfico, ellos hacen esto primeramente por medio de captura del tráfico bajo normales circunstancia llamado perfil. Se usa este perfil para comparar con el tráfico. Un perfil contiene información a cerca del diseño del tráfico y sus estadísticas. Cualquier tráfico que no concuerda con el perfil es considerado anormal y la red podría sufrir ataques ya que en este proceso el sistema del perfil muchas veces es llamado sistema de detección de anomalías.

Una de las principales ventajas del sistema basado en perfil es que tiene una mejor fluidez de detección en los nuevos ataques sobre los sistemas basados en asignaturas. Por ejemplo asume que un intruso descubre que existe un hoyo de seguridad en un Web Server y trata de acceder a un archivo especial llamado accesso.htm que ha sido dejado ahí por la instalación por defecto. Este archivo nunca puede ser referido pero este provee manejo de backdoor al Web Server . Normalmente este podría ser removido pero en algunos administradores podrían haber olvidado hacer esto. Este archivo nunca es accesado en operación normal, así que cuando un intruso prueba acceder a este archivo, el sistema basado en archivos podría caer en alarma ya que este tipo de actividades es considerado una anomalía.

Sistemas basados en Perfiles tiene algunos problemas detectando ataques sin embargo:

Están propensos a niveles altos de lectura falsas más que los sistemas de asignaturas porque los patrones de tráfico varían. Esto puede ser un problema cuando se introducen nuevas aplicaciones y dispositivos en la red de trabajo.

Además toma mas tiempo para determinar si un ataque realmente ocurre o si este fue una falsa lectura, incrementando el manejo de sobre saturación.
Debido al cambio en los patrones de tráfico y las topologías de la red, un gran tiempo debe ser invertido recreando un perfil actual incrementando su manejo.
Cuando se crea el perfila actual para compararlo con el tráfico, y si este perfil capturado incluye un ataque, entonces es tomado como tráfico normal, y si este ataque ocurre de nuevo y se compara con el perfil que contiene el ataque, el perfil IDS es considerado este normal y no cae en alerta, además muchas fases necesitan tener cuidado cuando se esta capturando perfiles de tráfico.

Características

El sistema basado en características compara el tráfico para detectar un ataque esta ocurriendo. Una característica es básicamente un grupo de criterios (comúnmente referidos como una plantilla) las soluciones de IDS podrían ser usadas cuando un ataque esta ocurriendo. El tráfico se compara con una lista de características y si este es igual una alarma se activará, este tipo de sistemas es comúnmente llamado detección indebida.

A diferencia del sistema basado en perfiles, el sistema de características tiene pocas lecturas falsas ya que ellos buscan cosas específicas en el tráfico. Como un ejemplo, si se conoce el mecanismo del acceso a un ataque de un web Server como la información contiene en un URL mal formado, una característica podría ver la especifica información en le segmento de la http.

Las soluciones de las características tienen dos principales desventajas:

Pueden detectar solo ataques que han sido programados en sus características de instalación. Si nuevos ataques son descubiertos hay una alta posibilidad que la característica de solución no podría detectar el ataque. Además se debe asegurar que las características de IDS siempre estén actualizadas las características de instalación.

Las características tienen problemas cuando están tratando con ataques horizontales que ocurren en un período de tiempo. Un buen intruso podría planear un reconocimiento y un acceso de ataque en un periodo largo de tiempo haciendo dificultoso su detección: imagine un ping un escaneo de puertos que ocurren sobre un período de horas o días con un perfil de sistema, esto probablemente podría debilitarse. Por otra parte una característica de solución basada en características no va a ser capaz de detectar este ataque porque no podría amortiguar todos los tráficos en un largo período de tiempo.

Complicaciones con los sistemas IDS

Cuando un sistema IDS detecta un ping o un escaneo de puertos en períodos largos reconoce estos ataques, puede observar docenas o cientos de paquetes que determina que el ataque esta ocurriendo. Para solucionar este tipo de ataques utilizando IDS podría ser la siguiente:

Indica que un ataque esta ocurriendo cuando realmente no hay un ataque
Perder un ataque por un intruso porque el ataque ocurre en un período de tiempo largo o porque el intruso esconde cuidadosamente entre los patrones de tráfico normal.

4.5.3 CONFIGURACIÓN DE IDS

El proceso de configuración requiere 3 pasos:

Paso 1: iniciación de la configuración
Paso 2: configuración de logging y postoffice
Paso 3: configuración y activación de reglas de auditoria

Paso 1 Iniciación de la configuración

Se debe configurar dos comandos básicos de iniciación de IDS:

```
Router(config)#ip audit po max-events #_de_eventos
Router(config)#ip audit smtp spam #_de_recipientes
```

El comando ip audit po max-events limita el número de eventos de IDS, que Cisco IOS puede enviar a un dispositivo remoto. Por defecto esto es 250 pero puede estar entre un rango de 1 a 65,535. Este límite puede ser usado para asegurar si un intruso puede saturar el router con muchos ataques, el router no podría ser sobresaturada en tratar de procesar todos ellos. Por otro lado, esto básicamente podría evitar que el intruso cree un ataque DoS contra el mismo router.

El comando ip audit smtp spam es usado para limitar el e-mail spamming que usan correos masivos, con este comando el número por defecto de recipientes permitidos es de 250. Si un mensaje se correo contiene más de este valor, el router ataca la acción configurada. El número de recipientes puede estar entre el rango de 1 a 65,535.

Paso 2 Configuración Loggin y Postoffice

La IOS Cisco puede usar dos métodos para eventos loggin IDS: la información log usa el syslog o la información usando un directorio IDS. Usando el syslog y IOS de Cisco puede la información log ser local o remotamente, y si se quiere utilizar el método de syslog se debe configurar el siguiente comando IDS:

```
Router(config)#ip audit notify log
```

Paso 3 Configuración y activación de reglas de auditoria

Cuando se ha definido el método logging se puede crear las reglas de auditoría IDS, dos grupos de comandos son usados para configurar estas reglas:

Políticas globales:

Son usadas para tomar las acciones apropiadas para igualar las características, al menos que otra regla específica designe otra cosa, para crear una política global usa los siguientes comandos:

```
Router(config)# ip audit info {action [alarm] [drop] [alarm]}
Router(config)# ip audit attack {action [alarm] [drop] [alarm]}
```

Como se puede observar los comandos especifican acciones para información y ataques de características. Cada uno tiene tres posibles acciones que el router pueden tomar:

Genera una alarma (log) donde esta es la acción por defecto, rechaza el paquete para la conexión TCP y baja la conexión.

Estos comandos son configurados solo si se desea cambiar la configuración por defecto de alarma.

Políticas específicas.

Se puede crear una categoría específica de políticas de IDS, típicamente se hace esto si se tiene dos interfaces en el router al lado una conexión de Internet y en otro lado un sitio remoto, si se quiere setear una política diferente IDS para cada interface se muestra el siguiente comando:

```
Router(config)# ip audit name nombre_auditoria {info ! attack} [list estándar_acl#de_nombre ] [action
[alarm] [drop] [reset] ]
```

La primera diferencia entre este comando y los comandos globales es que se deben de dar un nombre a la política. Además se debe especificar la categoría ya sea la información o el ataque. Opcionalmente puedes especificar un número de estándar ACL o nombre. Con esta opción solo permites el recurso para la dirección IP en la

ACL el cual es usado para igualar el tráfico. Si no se realiza esta configuración tomara por defecto la política global.

Características de la política

Por defecto, todas las características están habilitadas. En algunos casos, sin embargo si se quiere deshabilitar uno o varias características, talvez por un número alto de positivos falsos se igualan, se puede deshabilitar una característica con el siguiente comando:

```
Router(config)# ip audit signature signature  #{disable !list standard ACL # or name
```

Se debe especificar el número de características que se quieren deshabilitar. La lista de parámetros especifica un ACL Standard. Si una igualdad en la característica ocurre y el recurso de la dirección IP iguala cualquiera de las entradas deny en el estándar ACL, entonces el router no toma acción, solo la entrada permit permitirá al router el funcionamiento para la configuración de la auditoria del IDS.

POSITIVOS FALSOS

Muchas soluciones IDS autorizan disparar la alarma en procesos informacional, como un pings o una zona de transferencia DNS. Este es muy usado si se tiene un fuerte control sobre este. De cualquier manera si estos son acontecimientos comunes en el network, esto se convierte más fácil para esconder un ataque real, insertando muchos falsos positivos.

Políticas de protección

Cuando una alarma IDS es generada porque una característica fue disparada, la alarma contiene una locación designada para la fuente y la dirección destino. IN, indica que la dirección es interna a la red, y OUT indica que este es externo a la red. Seguramente el router no sabe la diferencia del interno con el externo, se le debe especificar con la siguiente configuración:

Router(config)# ip audit po protected IP address [to IP address]

Política de activación

Después que se tiene definido la política de auditoria de IDS, se debe activar en una interfase (s) antes que el router use estas. Para este se debe usar la siguiente configuración:

Router(config)# interface type [slot_#/] port _#
Router(config)# ip audit audit_name { in ! out }

Se especifíca que la política esta activada en el inbound (en el limite) o outbound (fuera de limite) de una interfase. Si se quiere activar una política en ambas direcciones ejecuta el comando dos veces, especifica IN por un comando y OUT para el otro. Normalmente, se activan la política IDS INBOUND en un perímetro de interfase del router externo. Después se tiene activo las políticas IDS, el router comienza comparando paquetes con las características de su base de datos.

Verificación IDS

Después de tener configurado IDS en el router, se usa un comando con múltiples parámetros para verificar la configuración IDS.

Router(config)#show ip audit. {all │configuration │interfaces │ name audit_name │ sessions │ statistics }

(Ver demostración de configuración de técnica en cd-anexo: video #5: IDS)

4.6 NAT [7]

NAT (Network Address Translation) es el proceso que permite la traslación de direcciones privadas a públicas mediante la substitución o alteración de las direcciones IP o puertos en las cabeceras IP y TCP del paquete transmitido. Para que NAT funcione debemos disponer de un router que implemente NAT en alguna o varias de sus variantes: NAT estático, NAT dinámico y NAT por puertos (PAT).

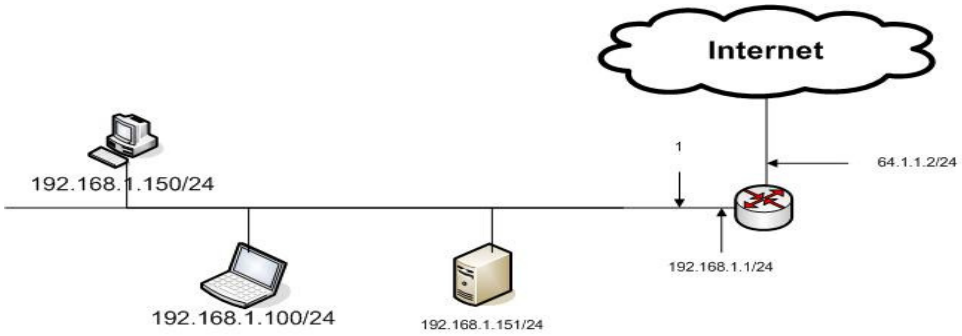


Figura 4.1 Ejemplo de red con la inclusión de la NAT

No siempre se usa NAT para trasladar direcciones privadas a públicas. Hay ocasiones en que se trasladan direcciones privadas a privadas o direcciones públicas a direcciones públicas. Por consiguiente se usa la siguiente nomenclatura genérica a la hora de usar NAT:

- Direcciones Internas (Inside addresses): aquellas direcciones que se quieren trasladar.
- Direcciones Externas (Outside addresses): son direcciones a las que se traslada las direcciones internas.

Las direcciones internas pueden ser tanto privadas como públicas. El caso más típico es aquel en que la dirección interna es una dirección privada y la dirección externa es una dirección pública. La clasificación anterior se puede subdividir a su vez:

- Direcciones locales internas (Inside local addresses): la dirección IP interna asignada a un host en al red interna.

- Direcciones globales internas (Inside global addresses): la dirección IP de un host en la red interna tal como aparece a una red externa.
- Direcciones locales externas (Outside local addresses): la dirección IP de un host externo tal como aparece a la red interna
- Direcciones globales externas (Outside global addresses): la dirección IP asignada a un host externo en una red externa.

Ver que la diferencia entre una dirección local y global interna es que la dirección local interna es la dirección que queremos trasladar mientras que la dirección global interna es la dirección ya trasladada.

(Ver demostración de configuración de técnica en cd-anexo: video #7: NAT)

4.7 TÉCNICAS DE ENCRIPTADO

4.7.1 REDES VIRTUALES PRIVADAS (VPN) [7]

INTRODUCCIÓN

Debido al crecimiento de las redes y las forma tan facil y practica de utilizar, como servicios al alcance de todos, las empresas y usuarios tienen otro punto de vista a la hora de implementar la interconexion de redes privadas de datos. Actualmente, estas redes privadas y la infraestructura de internet estan operando en paralelo. Sin embargo, todas las ventajas y beneficios ofrecidos a los proveedores de servicio y los usuarios finales, esta provocando que estos universos paralelos convergan en el concepto de red privada virtual (VPN). Esta convergencia es debida principalmente a cuatro motivos:

1. La movilidad geográfica de puestos de trabajo esta llevando a las redes privadas a una situación ingestionable. Los usuarios precisan conexiones que les permitan el acceso desde cualquier lugar del mundo. Estas necesidades, unidas a las surgidas como consecuencia de la demanda de

telecomunicaciones a tiempo completo, estan aumentando drásticamente el número de oficinas remotas que una compañía debe interconectar. Como resultado, muchas redes privadas estan convirtiéndose en redes ingestionables e intratables.

2. La necesidad de interactuar en línea con los clientes y los proveedores esta añadiendo un nuevo nivel de complejidad, en el cual muchas redes privadas deben tratarse de una forma independiente para su correcta integración y aislamiento respecto al resto. Las redes individuales emplean normalmente diferentes protocolos, diferentes aplicaciones, diferentes portadoras y diferentes sistemas de gestión de red. Esta escasez de denominadores comunes supone que la interacción de dos redes privadas se convierte en un reto aún mucho mayor.
3. El deseo de consolidar y simplificar la interfaz de usuario se ha convertido en un imperativo de negocio, dado que los usuarios son incapaces de defenderse en muchas de las nuevas aplicaciones.
4. El alto costo necesario para implementar y mantener redes privadas esta llevando a estas a una situación insostenible. Las líneas de larga distancia, así como los servicios conmutados, representan una serie de necesidades diarias. El personal de soporte necesario para gestionar las tecnologías complejas conlleva un crecimiento continuo tanto en el número de personas como en su experiencia. Igualmente, la dependencia de aplicaciones de red requiere un provisionamiento separado de backup además de una expansión de la infraestructura de la red privada ya existentes.

4.7.2 IPSEC

IPSEC es un estándar que proporciona servicios de seguridad a la capa IP y a todos los protocolos superiores basados en IP (TCP y UDP, en otros). Este estándar aborda las carencias en cuanto a seguridad del protocolo IP. Dichas carencias son muy graves y tal como se ha constatado en los últimos años, afectan a la infraestructura misma de las redes IP.
Todas las soluciones anteriores se basaban en soluciones propietarias que dificultaban la comunicación entre los distintos entornos empresariales, al ser necesario que estos dispusiesen de una misma plataforma.

La falta de interoperabilidad ha sido el principal freno para el establecimiento de comunicaciones seguras, dado que no se ve factible la migración a una determinada plataforma en función de una colaboración empresarial puntual.

4.7.2.1 VENTAJAS DE IPSEC

Entre estas destacan, que esta apoyado en estándares del IETF y que proporciona un nivel de seguridad común y homogéneo para todas las aplicaciones, además de ser independiente de la tecnología física empleada. IPSEC se integra en la version actual de IP (IP version 4) y lo que es todavia mas importante, se incluye por defecto en IPv6. Puesto que la seguridad es un requisito indispensable para el desarrollo de las redes IP, IPSEC esta recibiendo un apoyo considerable: todos los equipos de comunicaciones lo incorporan, asi como las últimas versiones de los sistemas operativos mas comunes. Al mismo tiempo, ya existen muchas experiencias que demuestran la interoperabilidad entre fabricantes, lo cual constituye una garantía para los usuarios.
Otra característica destacable de IPSEC es su carácter de estándar abierto. Se complementa perfectamente con la tecnología PKI y aunque establece ciertos algoritmos comunes, por razones de interoperabilidad, permite integrar algoritmos criptográficos mas robustos que pueden ser diseñados en un futuro.

4.7.2.2 BENEFICIOS QUE APORTA IPSEC

Posibilita nuevas aplicaciones como el acceso seguro y transparente de un nodo IP remoto.
Facilita el comercio electrónico de negocio a negocio, al proporcionar una infraestructura segura, sobre la cual se puedan realizar transacciones usando cualquier aplicación. Las extranets son un ejemplo.
Permite construir una red corporativa segura sobre redes públicas, eliminando la gestión y el costo de líneas dedicadas.

Ofrece al teletrabajador el mismo nivel de confidencialidad que dispondría en la red local de su empresa, no siendo necesaria la limitación de acceso a la información sensible por problemas de privacidad en tránsito.
Es importante señalar que cuando se hace referencia a la palabra “seguro” no se limita únicamente a la confidencialidad de la comunicación, también se hace referencia a la integridad de los datos, que para muchas compañías y entornos de negocio puede ser un requisito mucho más crítico que la confidencialidad.

Esta integridad es proporcionada por IPSEC como servicio añadido al cifrado de datos o como servicio independiente.
IPSEC es, en realidad, un conjunto de estándares para integrar en IP funciones de seguridad basadas en criptografía. Proporciona confidencialidad, integridad y autenticidad de datagramas IP, combinando tecnologías de clave pública (RSA), algoritmos de cifrado (DES, 3DES, IDEA, Blowfish), algoritmos de Hash (MD5, SHA-1) y certificados digitales X509v3.
El protocolo IPSEC ha sido diseñado de forma modular, de modo que se pueda seleccionar el conjunto de algoritmos deseados sin afectar a otras partes de la implementacion. Han sido definidos, sin embargo, ciertos algoritmos estándar que deberan soportar todas las implementaciones para asegurar la interoperabilidad en el mundo global de Internet. Dichos algoritmos de referencia son DES y 3DES, para cifrado, asi como MD5 y SHA-1, como funciones de Hash. Además es perfectamente posible usar otros algoritmos que se consideren más seguros o más adecuados para

un entorno específico: por ejemplo, como algoritmo de cifrado de clave simétrica IDEA, Blowfish o el más reciente AES que se espera sea el más utilizado en un futuro próximo.

4.7.2.3 IPSEC SE DISTINGUEN POR LOS SIGUIENTES COMPONENTES

Dos protocolos de seguridad. IP Authentication Header (AH) e IP Encapsulating Security Payload (ESP) que proporcionan mecanismos de seguridad para proteger tráfico IP.
Un protocolo de gestión de claves Internet Key Exchange (IKE) que permite a dos nodos negociar las claves y todos los parámetros necesarios para establecer una conexión AH o ESP.

4.7.2.3.1 EL PROTOCOLO AH

El protocolo AH es el procedimiento previsto dentro de IPSEC para garantizar la integridad y autenticación de los datagramas IP. Proporcionando un medio al receptor de los paquetes IP para autenticar el origen de los datos y para verificar que dichos datos no han sido alterados en tránsito. Sin embargo no proporciona ninguna garantía de confidencialidad, es decir, los datos transmitidos pueden ser vistos por terceros. Tal como indica su nombre, AH es una cabecera de autenticación que se inserta entre la cabecera IP estándar (tanto IPv4 como IPv6) y los datos transportados, que pueden ser un mensaje TCP, UDP o ICMP o incluso un datagrama IP completo.

Versión	Hlen	TOS	Longitud Total	
Identificación			Flags	Offset
TTL		Protocolo = 50	Checksum	
Dirección IP Origen				
Dirección IP Destino				
Siguiente encabezado		Largo de carga	Reservado	
Índice de parámetros de seguridad (SPI)				
Número de secuencia				
Capa de autenticación				
TCP				
Datos de aplicación				

Tabla 4.1 Formato de protocolo AH

AH es realmente un protocolo IP nuevo y como tal el IANA (Internet Assigned Numbers Authority / Autoridad que asigna Números de Internet) le ha asignado el número decimal 51. Esto significa que el campo protocolo de la cabecera IP contiene el valor 51, en lugar de los valores 6 o 17 que se asocian a TCP y UDP respectivamente. Es dentro de la cabecera AH donde se indica la naturaleza de los datos de la capa superior. Es importante destacar que AH asegura la integridad y autenticidad de los datos transportados y de la cabecera IP, excepto los campos variables: TOS, TTL, flags, offset y checksum.

El funcionamiento de AH se base en un algoritmo HMAC, esto es; un código de autenticación de mensajes. Este algoritmo consiste en aplicar una función Hash a la combinación de unos datos de entrada y una clave, siendo la salida una pequeña cadena de caracteres que denominados extracto. Dicho extracto tiene la propiedad de que es como una huella personal asociada a los datos y la persona que lo ha generado, puesto que es la única que conoce la clave.

En la siguiente figura se muestra el modo en que funciona el protocolo AH.

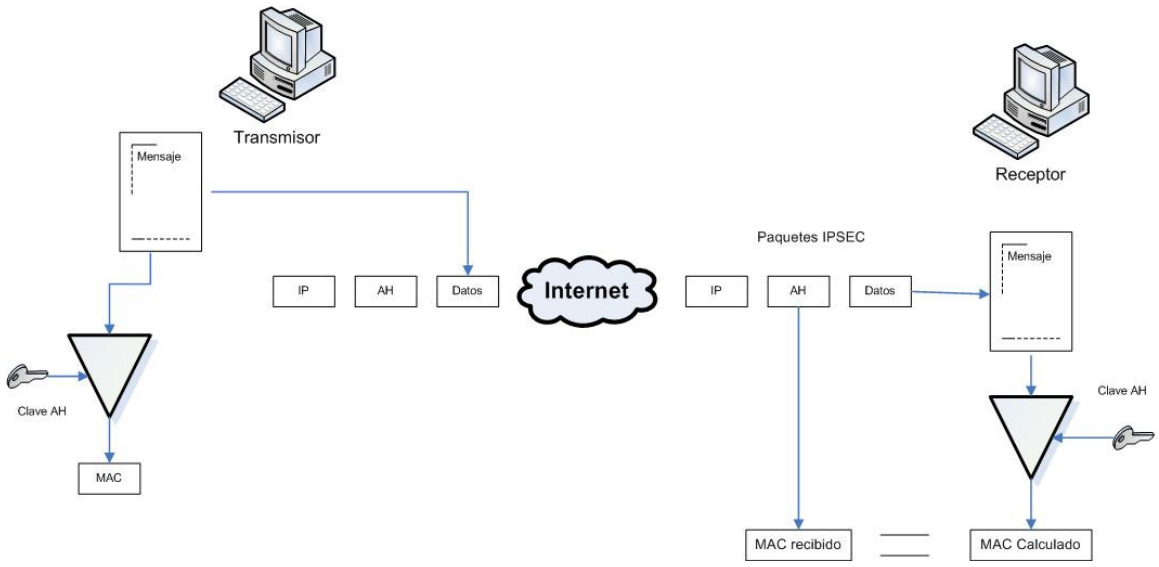


Figura 4.2 Fucionamiento del protocolo AH

4.7.2.3.2 FUNCIONAMIENTO AH

El emisor calcula un extracto del mensaje original, el cual se copia en uno de los campos de la cabecera AH. El paquete asi construido se envia atraves de la red, repitiendose en el extremo receptor el cálculo del extracto y comparandolo con el recibido en el paquete. Si son iguales, el receptor tiene la seguridad de que el paquete IP no ha sido modificado en tránsito y que procede efectivamente del origen esperado.

4.7.2.3.3 EL PROTOCOLO ESP

El objetivo principal del protocolo ESP (Encapsulating Security Payload) es proporcionar confidencialidad, para ello especifíca el modo de cifrar los datos que se desean enviar y como este contenido cifrado se incluye en un datagrama IP. Adicionalmente, puede ofrecer los servicios de integridad y autenticación del origen de los datos incorporando un mecanismo similar al de AH.

Dado que ESP proporciona más funciones que AH, el formato de la cabecera es más complejo; este formato consta de una cabecera y una cola que rodean los datos

transportados. Dichos datos pueden ser cualquier protocolo IP (por ejemplo, TCP, UDP o ICMP o incluso un paquete IP completo). En la siguiente figura se muestra la estructura de un datagrama ESP, en la que se observa como el contenido o carga útil viaja cifrada.

Versión	Hlen	TOS	Longitud Total	
Identificación			Flags	Offset
TTL		Protocolo = 50	Checksum	
Dirección IP Origen				
Dirección IP Destino				
Siguiente encabezado		Largo de carga	Reservado	
Índice de parámetros de seguridad (SPI)				
Número de secuencia				
Capa de autenticación				
TCP				
Datos de aplicación				
Campo de autenticación				

Tabla 4.3 Estructura de la trama ESP

El IANA (Internet Assigned Numbers Authority / Autoridad que asigna Números de Internet) ha asignado al protocolo ESP el número decimal 50. Esto implica que el campo Protocolo de la cabecera IP contendra el valor 50, mientras que dentro del mensaje ESP se indica la naturaleza de los datos. Puesto que este campo, al igual que la carga útil, esta cifrado, un hipotético atacante que intercepte el paquete no podra saber si el contenido es TCP o UDP; esto es completamente normal ya que el objetivo que se persigue es, precisamente, ocultar la información.

La función de cifrado dentro del protocolo ESP es desempeñada por un algoritmo de cifrado de clave simétrica. Típicamente se usan algoritmos de cifrado bloque, de modo que la longitud de los datos a cifrar tiene que ser un múltiplo del tamaño de bloque (8 o 16 byte, en la mayoria de los casos). Por está razón existe un campo de relleno, el cuál tiene una función adicional: es posible añadir caracteres de relleno al campo de datos para ocultar así su longitu real y por tanto, las características del tráfico. Un atacante suficientemente hábil podría deducir cierta información a partir del análisis de ciertos parámetros de las comunicaciones, aunque esten cifradas, tales como el retardo entre paquetes y su longitud. La función de relleno esta pensada para dificultar este tipo de ataques.

A continuación se presenta como el protocolo ESP permite enviar datos de forma confidencial.

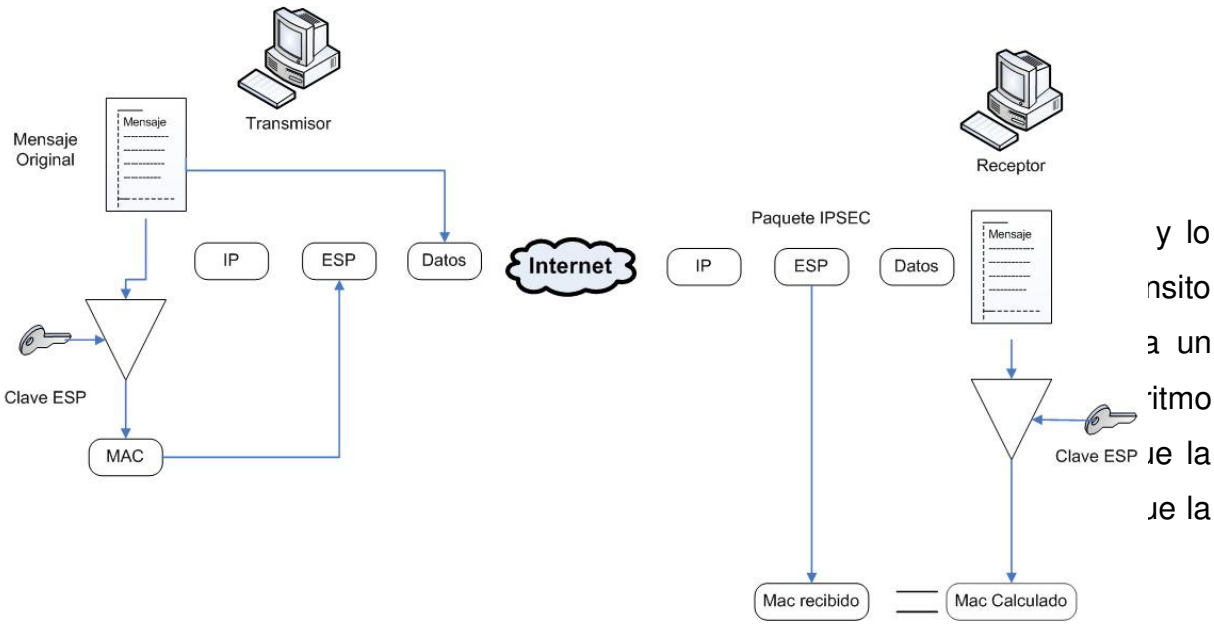


Figura 4.3 Funcionamiento del protocolo ESP

4.7.2.3.4 FUNCIONAMIENTO ESP

La distribución de claves de forma segura es, por consiguiente, un requisito esencial para el funcionamiento de ESP y tambien de AH, como hemos visto anteriormente. Asimismo, es fundamental que el emisor y el receptor esten de acuerdo tanto en el algoritmo de cifrado o de Hash y como en el resto de parámetros comunes que utilizan. Esta labor de puesta en contacto y negociación es realizada por un protocolo de control, denominado IKE.

4.7.2.3.5 LOS MODOS DE TRANSPORTE Y DE TUNEL

Antes de entrar en los detalles del protocolo IKE es necesario explicar los dos modos de funcionamiento que permite IPSEC. Tanto ESP como AH proporcionan dos modos de uso:

EL MODO TRANSPORTE

En este modo el contenido transportado dentro del datagrama AH o ESP son datos de la capa de transporte (por ejemplo, datos TCP o UDP). Por tanto, la cabecera IPSEC se inserta inmediatamente a continuación de la cabecera IP y antes de los datos de los niveles superiores que se desean proteger. El modo transporte tiene la ventaja de que asegura la comunicación extremo a extremo, pero requiere que ambos extremos entiendan el protocolo IPSEC.

EL MODO TUNEL

En este el contenido del datagrama AH o ESP es un datagrama IP completo, incluida la cabecera IP original. Asi, se toma un datagrama IP al cuál se añade inicialmente una cabecera AH o ESP, posteriormente se añade una nueva cabecera IP que es la que se utiliza para encaminar los paquetes através de la red. El modo tunel se usa normalmente cuando el destino final de los datos no coinciden con el dispositivo que realiza las funciones IPSEC.

El modo tunel es empleado principalmente por los gateways IPSEC, con objeto de identificar la red que protegen bajo una misma direccion IP y centralizar de este modo el procesado del tráfico IPSEC en un equipo. El modo tunel también es útil, cuando se utiliza junto con ESP, para ocultar la identidad de los nodos que se estan comunicando. Otra aplicación del modo tunel, tanto con ESP como con AH, es poder establecer Redes Privadas Virtuales (VPN por sus siglas en ingles) atraves de redes publicas, es decir, interconectar de forma segura redes de area local, incluso en el caso de que estas usen direccionamiento privado o no legal en Internet.

IPSEC puede ser implementado bien en un host o bien en un equipo dedicado, tal como un enrutador o un Firewall, que cuando realiza estas funciones se denomina gateway IPSEC.

A continuación se muestra los dos modos de funcionamiento del protocolo IPSEC.

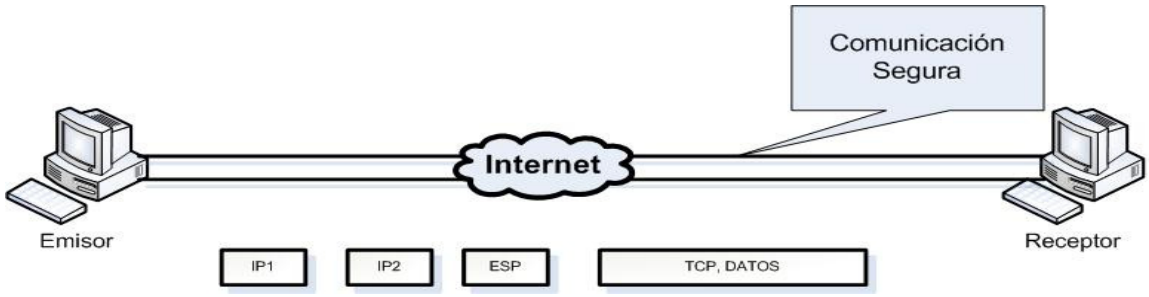


Figura 4.4 Representación del Modo transporte

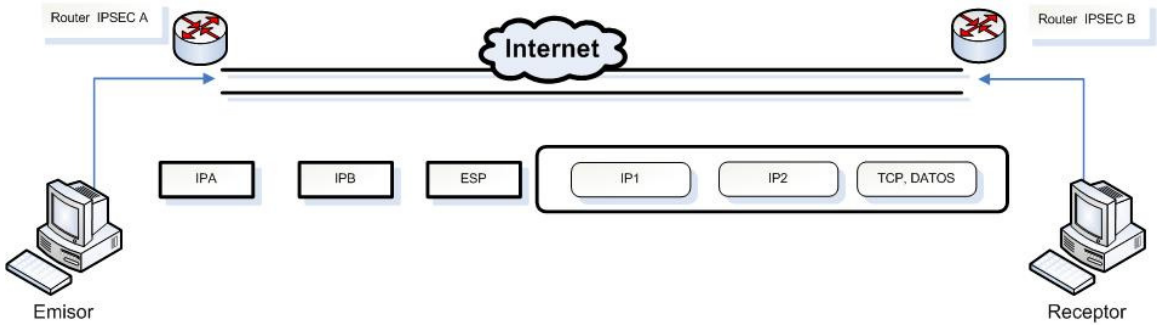


Figura 4.5 Representación del Modo túnel

4.7.2.3.6 IKE EL PROTOCOLO DE CONTROL

Un concepto esencial en IPSEC es el de asociación de seguridad (SA): es un canal de comunicación unidireccional que conecta dos nodos, a través del cual fluyen los datagramas protegidos mediante mecanismos criptográficos acordados previamente. Al identificar únicamente un canal unidireccional, una conexión IPSEC se compone de dos SAAs, una por cada sentido de la comunicación.

Hasta el momento se ha supuesto que ambos extremos de una asociación de seguridad deben tener conocimiento de las claves, así como del resto de la información que necesitan para enviar y recibir datagramas AH o ESP. Tal como se ha indicado anteriormente, es necesario que ambos nodos esten de acuerdo tanto en los algoritmos criptográficos a emplear como en los parámetros de control. Esta operación puede realizarse mediante una configuración manual o mediante algún protocolo de control que se encargue de la negociación automática de los parámetros necesarios; a esta operación se le llama negociación de SSAs. El IETF ha definido el protocolo IKE para realizar tanto esta función de gestión automática de claves como el establecimiento de las SSAs correspondientes. Una característica importante de IKE es que su útilidad no se limita a IPSEC, sino que es un protocolo estándar de gestión de claves que podría ser útil en otros protocolos, como por ejemplo, OSPF o RIPV2. IKE es un protocolo híbrido que ha resultado de la integración de dos protocolos complementarios: ISAKMP y Oakley.
ISAKMP define de forma generica el protocolo de comunicación y la sintaxis de los mensajes que se utilizan en IKE, mientras que Oakley especifica la lógica de como se realiza de forma segura el intercambio de una clave entre dos partes que no se conocen previamente.

El objetivo principal de IKE consiste en establecer una conexión cifrada y autenticada entre dos entidades, a través de la cuál se negocian los parámetros necesarios para establecer una asociación de seguridad IPSEC. Dicha negociación se lleva a cabo en dos fases:

La fase común a cualquier aplicación, en la que ambos nodos establecen un canal seguro y autenticado. Dicho canal seguro se consigue mediante el uso de un algoritmo de cifrado simétrico y un algoritmo HMAC. Las claves necesarias se derivan de una clave maestra que se obtiene mediante un algoritmo de intercambio de claves Diffie-Hellman. Este procedimiento no garantiza la identidad de los nodos, para ellos es necesario un paso adicional de autenticación.

Existen varios métodos de autenticación, los dos más comunes se describen a continuación:

1. El primer método de autenticación se basa en el conocimiento de un secreto compartido que, como su propio nombre indica, es una cadena de caracteres que únicamente conocen los dos extremos que quieren establecer una comunicación IPSEC. Mediante el uso de funciones Hash cada extremo demuestra al otro que conoce el secreto sin revelar su valor; así los dos se autentican mutuamente. Para no debilitar la seguridad de este mecanismo de autenticación, debe configurarse un secreto distinto para cada par de nodos, por lo que el número de secretos crece muy rápidamente cuando aumenta el número de nodos. Por esta razón en entornos en los que se desea interconectar muchos nodos IPSEC la gestión de claves es muy complicada. En este caso no se recomienda el uso de autenticación mediante secreto compartido, sino autenticación basada en certificados digitales.
En los estándares IPSEC esta previsto el uso de un método de autenticación que se basa en utilizar certificados digitales X509v3. El uso de certificados permite distribuir de forma segura la clave pública de cada nodo, de modo que ese puede probar su identidad mediante la posesión de la clave privada y ciertas operaciones de criptografía pública. La utilización de certificados requiere de la aparición de un elemento más en la arquitectura IPSEC, la PKI (Infraestructura de Clave Pública).

2. La segunda fase es el canal seguro IKE, es usado para negociar los parámetros de seguridad específicos asociados a un protocolo determinado, en nuestro caso IPSEC. Durante esta fase se negocian las características de la conexión ESP o AH y todos los parámetros necesarios. El equipo que ha iniciado la política de seguridad y

con la prioridad que se hayan configurado. El sistema receptor aceptará la primera que coincida con los parámetros de seguridad que tenga definidos. Así mismo, ambos host se informan del tráfico que van a intercambiarse através de dicha conexión.

4.7.2.4 APLICACIONES PRÁCTICAS DE IPSEC

La tecnología IPSEC permite construir soluciones de comunicaciones que ofrecen confidencialidad y autenticación en la capa IP, independientemente de cual sea el medio de transporte (FR, PPP, xDSL o ATM). Además, la inclusión de seguridad en la capa IP tiene la ventaja de que se extiende universalmente, ofreciendo un nivel de seguridad homogéneo de manera independiente del tipo que sean las aplicaciones, siempre que esten basadas en IP.

1.- Interconexión segura de redes locales.
2.- Acceso seguro de usuarios remotos.
3.- Extranet o conexión de una corporación con sus distribuidores y proveedores.

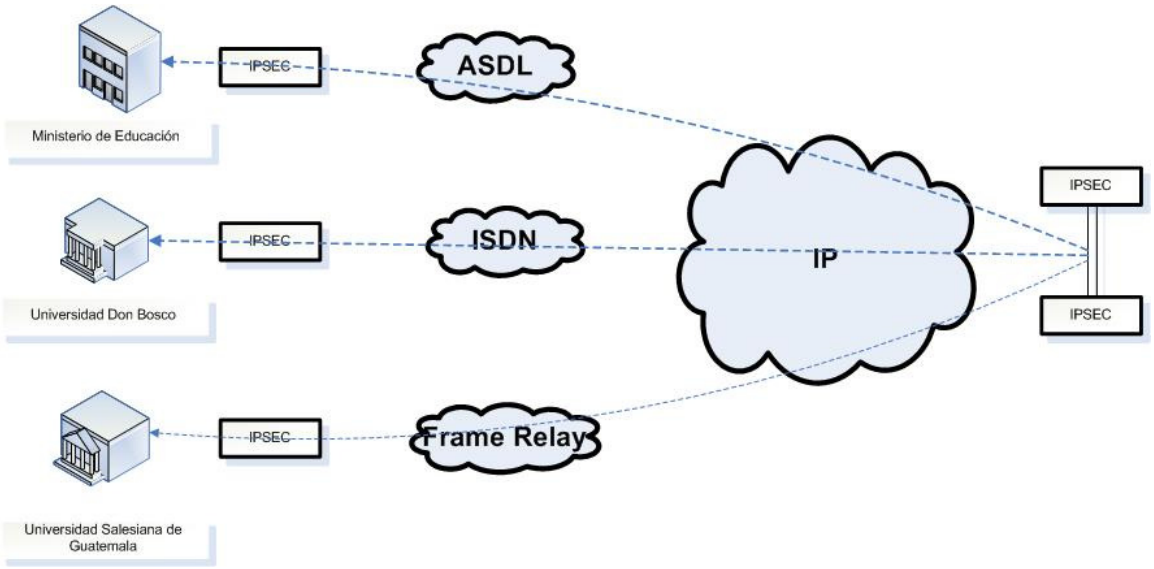


Figura 4.6 Ejemplo de soluciones viables para diferentes escenarios.

Para cada uno de los escenarios mostrados en la figura 4.6 se desarrolla una aplicación práctica concreta y se presentan las ventajas de utilizar IPSEC.

La mayoría de las corporaciones utiliza IP como medio de transporte universal y las que todavía no usan IP tienen planes de migrar completamente a esta tecnología en un futuro próximo. Asi mismo, la naturaleza distribuida de las empresas hace necesaria una infraestructura de comunicaciones que interconecte todas sus oficinas o puntos de venta.

Por Intranet se entiende una red de comunicaciones basada en una infraestructura de comunicaciones públicas o privadas que conecta todos los puntos de trabajo de una empresa y que tiene como medio común IP.

Dicha Intranet conecta todas las oficinas bancarias con el centro de proceso de datos (CPD) de un gran banco. La seguridad es vital en este entorno y los requisitos de confidencialidad e integridad de las comunicaciones se cubren perfectamente mediante el uso de la tecnología IPSEC.

En la actualidad, incluso las oficinas bancarias mas pequeñas disponen de una infraestructura informática que consta de una red local con varios PCs que usan una

variedad de aplicaciones y protocolos para los que es imposible o muy costoso añadir mecanismos de seguridad. Sin embargo, todo el tráfico de ésta red local esta basado en IP o puede ser encapsulado en IP, de modo que la instalación de un gateway IPSEC es la mejor solución para garantizar la seguridad de las comunicaciones de la oficina con el exterior.

Es habitual que las oficinas bancarias, debido a su elevado número, presenten una gran diversidad de tecnologías de acceso. Para grandes bancos con presencia multinacional y oficinas dispersas en muchos países esta diversidad será mayor, de forma que incluso podría plantearse la conexión de algunas oficinas directamente através de Internet. En cualquier caso, IPSEC garantiza la protección de las comunicaciones con independencia de la tecnología de acceso empleada. En cuanto al centro de proceso de datos, los requisitos críticos son la fiabilidad y la capacidad para mantener un elevado número de sesiones simultáneas. En el mercado estan disponibles gateways IPSEC comerciales que incorporan la posibilidad de configuración redundante y el establecimiento de 25,000 túneles simultáneos o más. Estas prestaciones son suficientes incluso para las redes bancarias mas grandes.

El acceso seguro a los usuarios

La gran mayoría de las empresas necesitan proporcionar a sus usuarios algún procedimiento para el acceso remoto a los recursos corporativos. Estos usuarios con necesidades de acceso remoto pueden ser agentes de ventas, teletrabajadores o directivos en viaje de negocios; en todos los casos se requiere la necesidad de poder acceder de forma segura a los sistemas informáticos de la empresa a cualquier hora y en cualquier lugar, incluso en el extranjero. Además, las previsiones de futuro apuntan a que estas necesidades de acceso remoto van a crecer espectacularmente. La tecnología IPSEC permite comunicar el PC del usuario remoto a las máquinas del centro corporativo, de modo que se soporten todas las aplicaciones IP de forma transparente. Mediante la instalación de un software en el PC, denominado “cliente IPSEC”, es posible conectar remotamente dicho equipo móvil a la red local de la corporación de forma totalmente segura, con la ventaja de que el usuario remoto, desde cualquier lugar del mundo, del mismo modo que si estuviese físicamente en su oficina, podrá:

- Leer y enviar correos electronicos.
- Acceder a discos compartidos en red.
- Acceder al servidor Web corporativo.
- Consultar la agenda.

El uso del estándar IPSEC permite garantizar la confiencialidad y la autenticidad de las comunicaciones extremo a extremo, de modo que esta solución de acceso remoto se integra perfectamente con los sistemas de seguridad de la red corporativa.

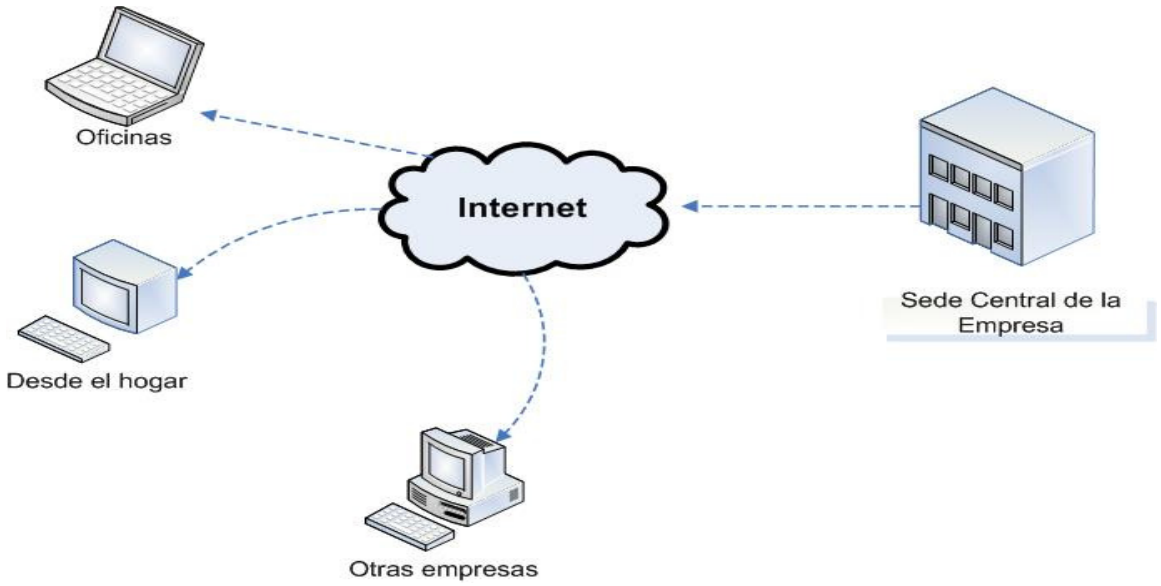


Figura 4.7 Escenario típico de acceso remoto seguro a una corporación

Dada la creciente competitividad en el sector informático, la protección de la propiedad intelectual, la información estratégica y de nuevos productos e incluso de la propia imagen de la empresa, imponen requisitos de control de acceso y de confidencialidad que hacen imprescindible la implementación de un sistema de acceso remoto que sea suficientemente seguro.

El protocolo IPSEC permite construir una solución que cumple estos requisitos de seguridad. En este entorno, los usuarios remotos dispondrán de un software instalado en su PC de trabajo que les permitirá establecer una conexión segura con la red local de la compañía. La variedad de sistemas operativos no supone dificultad alguna ya que todos los sistemas operativos recientes como Windows 2000 o Solaris 8 incluyen un cliente IPSEC. Asimismo, para los sistemas operativos más difundidos y que no integran IPSEC, existen aplicaciones de cliente IPSEC, tanto comerciales como de libre distribución. Incluso existe un cliente IPSEC para Palm Pilot. Para garantizar la seguridad de esta solución y evitar intrusiones, como las que han afectado a Microsoft y otras corporaciones en el pasado, es necesario complementar la tecnología IPSEC con el uso, en los equipos remotos, de firewall personales y

autenticación fuerte mediante certificados digitales X.509 residentes en tarjetas inteligentes.
Desde el punto de vista del administrador de la red informática de la corporación, los requisitos prioritarios serán la facilidad de gestión y la necesidad de autenticar de forma fiable a cada usuario. La integración de IPSEC con una infraestructura de clave pública (PKI) proporciona una respuesta adecuada a estos requisitos.

La Extranet

Por Extranet se entiende una red de comunicaciones que interconecta a una empresa con todos los agentes con los cuales mantiene relaciones comerciales: consumidores, proveedores y distribuidor. En este escenario la interoperabilidad que ofrece el estándar IPSEC es una ventaja clave frente a otras soluciones; cada empresa comprará equipos de fabricantes distintos, pero todos ellos podran conectarse de forma segura utilizando IPSEC como lenguaje común.

La tendencia actual es la aparición de Extranets en las que convergen todas las empresas que participan en un mismo sector productivo. Previsiblemente, el comercio electrónico negocio a negocio (B2B) evolucionará en este sentido, para proporcionar puntos de encuentro virtuales en los que se establezcan relaciones comerciales de empresa a empresa de forma segura.
Estos mercados virtuales especializados se articularán de forma natural en torno a la elaboración de un producto o la provisión de un servicio concreto: fabricación del automóvil y el tipo de industria que lleva asociada, distribución y comercialización de alimentos, sector asegurador, etc.

Para el caso, un ejemplo claro sería dos puntos de red distantes el uno del otro, los cuales se pueden comunicar de forma segura para intercambiar información.
Este es un ejemplo claro en el que IPSEC aparece como la solución mas apropiada, dado que es una tecnología avalada por estándares internacionales, garantiza la interoperabilidad entre los equipos de distintos fabricantes y proporciona el más alto nivel de seguridad gracias a las técnicas criptográficas más modernas.

Una extranet como esta puede llevarse a cabo perfectamente usando IPSEC; para ello se requiere la instalación de un gateway IPSEC en cada uno de los puntos de presencia de la extranet, mientras que el equipamiento de los usuarios se reduce a una PC portátil con un cliente IPSEC.

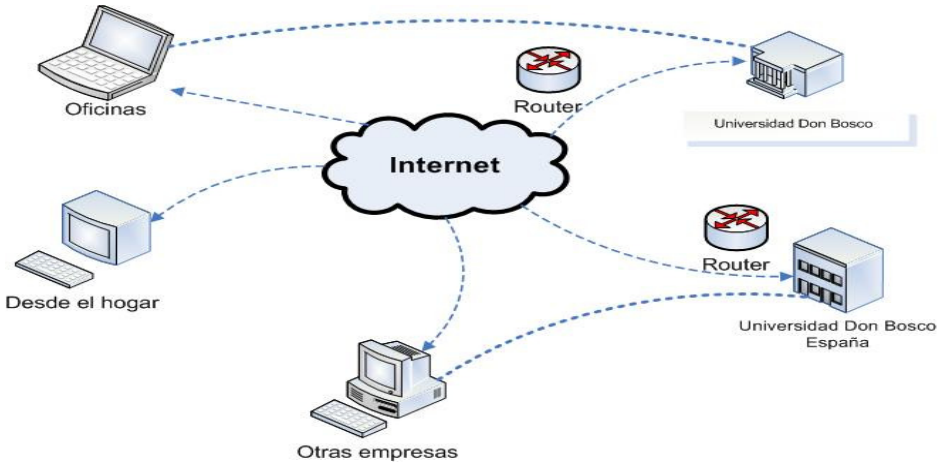


Figura 4.8 Intercambio de información entre dos compañias de forma segura

Firewall

Se sabe que el Firewall es una herramienta exclusivamente desarrollada para la seguridad de las redes y la protección de los sistemas interconectados. Sin embargo este sistema tiene también implicaciones en lo que a redes virtuales respecta ya que permite la posibilidad de ejecutar software que realice conexiones con diferentes redes privadas en Internet. Para ello, es necesario el establecimiento de líneas virtuales por las cuales los datos intercambiados viajen encriptados y autenticados (por ejemplo empleando IPSEC).

No obstante, no todo son ventajas. Así, por el momento no es posible disponer de un Proxy genérico que sea capaz de soportar todos los servicios, sino que cada servicio dispone de su Proxy (http-proxy, ftp-proxy, etc). Además, los Proxis no son mecanismos transparentes dado que las aplicaciones deben configurarse para que establezcan su conexión al Firewall en lugar de a los servidores externos.

En la práctica, los Firewall son combinaciones entre las técnicas de filtrado a nivel IP, a nivel de aplicación y a nivel de conexión. La determinación de estas técnicas dependerá del nivel de flexibilidad, transparencia, y seguridad requerida.

Entre los diferentes algoritmos empleados cabe destacar RADIUS y TACACS+ para realizar la autenticación y la autorización y DES, 3-DES y Diffie-Hellman para llevar a cabo la encriptacion.

4.7.3 REQUERIMIENTOS BÁSICOS DE UNA VPN

- Por lo general cuando se desea implementar una VPN hay que asegurarse que esta propocione:

- Identificación de usuario
- Administración de direcciones
- Codificación de datos
- Administración de claves
- Soporte a protocolos múltiples

- La VPN debe ser capaz de verificar la identidad de los usuarios y restringir el acceso a la VPN a aquellos usuarios que no estén autorizados. Así mismo, debe proporcionar registros estadísticos que muestren quién accesó, que información y cuándo.

- Administración de direcciones. La VPN debe establecer una dirección del cliente en la red privada y debe cerciorarse que las direcciones privadas se conseven así.

- Codifciación de datos. Los datos que se van a transmitir através de la red pública deben ser previamente encriptados para que no puedan ser leídos por clientes no autorizados de la red.

- Administración de claves. La VPN debe generar y renovar las claves de codificación para el cliente y el servidor.

- Soporte a protocolos múltiples. La VPN debe ser capaz de manejar los protocolos comunes que se utilizan en la red pública. Estos incluyen el protocolo de Internet (IP), el intercambio de paquete de Internet (IPX) entre otros.

4.7.4 VENTAJAS DE UNA VPN

Dentro de las ventajas más significativas se puede mencionar:

- La integridad
- Confidencialidad
- Seguridad de los datos
- Reducción de costos
- Sencilla de usar
- Sencilla instalación del cliente en cualquier PC Windows
- Control de Acceso basado en políticas de la organización
- Herramientas de diagnóstico remoto
- Los algoritmos de compresión optimizan el tráfico del cliente
- Evita el alto costo de las actualizaciónes y mantenimiento a las PC's remotas

4.7.5 TIPOS DE VPN

Acceso de usuario remoto a través de Internet: Las VPNs deben proporcionar acceso remoto a los usuarios de la corporación atraves de Internet y al mismo tiempo conservar la privacidad de la información.

En vez de tener que utilizar una línea alquilada o hacer una llamada de larga distancia a un servidor de acceso a red corporativo o externo (NAS), el usuario debe llamar a un número telefónico local NAS de ISP, posteriormente, el programa de la VPN crea una red privada virtual entre el usuario que marca y el servidor corporativo de VPN a través de Internet.

Conexión de redes atraves de Internet: Existen dos métodos para utilizar las VPNs y permitir la conexión de las redes de área local a sitios remotos:

a) Uso de líneas dedicadas para conectar una sucursal LAN corporativa: En este caso, tanto los enrutadores de la sucursal como los de la central corporativa pueden utilizar una línea dedicada local y el ISP local para conectarse a Internet. El software de la VPN utiliza las conexiones de ISP locales e Internet pública para crear una red privada virtual entre el enrutador de la sucursal y el enrutador corporativo.

b) Uso de una línea de marcación para conectar una sucursal a una LAN corporativa: En este caso, el enrutador en la sucursal puede llamar al ISP local. El software de la VPN utiliza la conexión al ISP local para crear una red privada virtual entre el enrutador de la sucursal y el enrutador de la central corporativa a través de internet.

c) Conexión de computadoras atraves de una Intranet: en algunas corporaciones, existen departamentos que debido a la informacion que manejan estan físicamente desconectados de la red interna de la corporación con el fin de proteger estos datos, pero a su vez, causa problemas de accesibilidad para aquellos usuarios que necesiten dicha información.

Para lograr el acceso a estos datos se debe realizar una VPN ya que esta va a permitir que la LAN del departamento esté físicamente conectada a la red interna corporativa y a su vez sperada por un servidor de VPN. Al utilizar una VPN, el administrador de la red puede asegurar que solo los usuarios autorizados de la red interna corporativa, pueden establecer una VPN con el servidor de VPN y lograr acceso a los recursos protegidos del departamento. Además, todas las comunicaciones a través de la VPN pueden encriptarse para lograr una mayor privacidad de los datos.

(Ver demostración de configuración de técnica en cd-anexo: video #11: VPN)

4.8 TÉCNICAS DE AUTENTICACIÓN

4.8.1 AUTENTICACIÓN PROXY (AP) [3]

AP es parte del conjunto de características de la IOS Cisco de Firewall y se requiere comprar el Software de la IOS Cisco adecuado para acceder a esta característica.
AP habilita la posibilidad de definir políticas de acceso de seguridad por usuario, las cuales se activan cuando un usuario se autentica para acceder al Router. Por ejemplo: puede ser que se desee denegar todo tipo de tráfico que entra a la red para abrir los temporales en el perímetro Router / Firewall para usuarios específicos. De seguro en muchos casos se puede saber desde que dispositivos los usuarios iniciarán sus conexiones de entrada.

AP puede tratar con estas situaciónes porque la IOS Cisco autentica usuarios y se basa en su autenticación, abre hoyos temporales configurando ACL en el Router para permitir que los usuarios accedan a los recursos temporales.

4.8.2 CARACTERÍSTICAS DEL AP

AP primero fue introducido en la versión IOS Cisco 12.0 (5) t. Sin embargo, fue limitado a desarrollar la autenticación por http: el usuario tuvo que usar la habilitación de Java para autenticar por Web Browser, desde entonces Cisco ha agregado soporte para otros métodos de autenticación:

HTTP-Cisco IOS 12.0(5) t.
HTTPS (usando SSL) – Cisco IOS 12.2 (11) y 12.2(15).
TELNET – Cisco IOS 12.3 (1).
FTP – Cisco IOS 12.3(1).

AP también soporta una forma de perfiles llamados ACL's o perfiles de acceso. AP requiere usar un servidor externo AAA que tenga las cuentas de usuarios y los perfiles de acceso configurados en el. Cuando un usuario se autentica

satisfactoriamente, el acceso al perfil de los usuarios es descargado al Router, donde la IOS Cisco incluye el acceso al perfil como entradas temporales ACL en las ACL estáticas del Router.

AP es compatible con muchas otras características de la seguridad de la IOS Cisco, incluyendo IDS, CBAC, NAT, IPSec y VPNs.

Si AP observa un número alto anormal de solicitudes HTTP, este puede indicar que el Router esta bajo un ataque DoS. AP puede limitar el número de estas respuestas abiertas y descartar cualquier solicitud. AP aunque trabaja con CBAC y NAT, de cualquier forma si se quiere usar AP y tener NAT configurado en el Router, Cisco requiere usar también CBAC.

Por ejemplo, un usuario puede usar AP para autenticación usando la dirección original, pero NAT traslada esta dirección a otra. Lo importante en esta situación es que se crea cualquier entrada ACL dinámica temporal, porque en AP la autenticación debería de tener la correcta información de direccionamiento. CBAC es necesaria aquí porque CBAC inspecciona el tráfico para asegurarse que las entradas ACL se creen de forma correcta para la autenticación de usuario.
AP esta integrado dentro de AAA, una buena característica de AP y AAA es que se puede generar el inicio y detener el record de autenticación para el tráfico que se origina desde que el usuario se autentica (esto requiere la configuración de atributos RADIUS y TACACS+ para servidor de conexiones.

Tabla 4.4 Características de AAA

Conexiones de Autenticación	Autenticación Proxy http, https, telnet y FTP
Conexiones de Usuarios	Pueden ser directamente conectado al Router (o con uno de los servicios antes mencionados)
Método de Autenticación	Autentica AAA y Autorización con RADIUS o TACACS+
ACL Localmente Temporales	Definido en el servidor AAA y descargado al Router
Entradas ACL Temporales	Cada usuario o grupo puede tener este acceso propio al perfil

4.8.3 USO DE AUTHENTICATION PROXY

Al momento de utilizar AP hay que decidir qué método de autenticación se utilizará; para el caso se tienen los siguientes: HTTP, HTTPS, TELNET y FTP. Normalmente se recomienda el uso de HTTPS porque la conexión es cifrada. Lo que se pretende con el uso de AP es proveer de un método de acceso más seguro.

Para prever la autentificación segura, el AP utiliza Javascript. Esto se asegura de que el nombre de usuario y la contraseña sean enviados al router en vez de ser enviado a otro WEB Server. Por lo tanto, el Cisco recomienda altamente que el Javascript esté permitido para las conexiones de HTTP/HTTPS.

Sin embargo, el AP permite la autentificación sin Javascript, especialmente en los sitios que se ha inhabilitado Java debido a razones de seguridad. Si el Javascript es desactivado, cuando el usuario procura la conexión hacia la WEB y el router la intercepta, una ventana pop-up se abriría en el escritorio del usuario que contiene el siguiente:
Instrucciones en cómo permitir a Javascript realizar el proceso de la autentificación automáticamente, Instrucciones de cómo terminar manualmente el proceso de autenticación y cómo establecer la conexión Web del usuario.

4.8.4 CUANDO USAR AP

AP realmente tiene muchas aplicaciones prácticas. AP prueba su utilidad para arreglos en la seguridad en estas situaciónes:
Necesita autenticar y autorizar usuarios externos antes de permitirles el acceso a específicos recursos internos, como un Servidor Web apropiado.
Necesita autenticar y autorizar usuarios internos antes de permitirles acceso a la extranet o recursos de Internet.
Se quiere realzar la configuración de la VPN, pre-autenticado usuarios antes de permitirles que configuren una conexión VPN en el Router.

Necesita configurar diferentes niveles de acceso en base por usuario, pero no se sabe necesariamente la dirección IP del usuario porque estas pueden cambiar cada día (probablemente porque ellos usen PPP o DHCP para adquirir su información de direccionamiento).
Necesita en detalle la intervención de quien se conecta a través del Router, el tiempo en el que se esta conectado y cuando sucedieron estas conexiones.

4.8.5 DONDE USAR AP

Se puede configurar simultáneamente las políticas que permitan por medio de AP que un usuario externo sea autenticado y autorizado para acceder a recursos internos, así como los usuarios internos acceden a los recursos externos.

4.8.6 LIMITACIONES DE AP

A pesar de sus ventajas, AP tiene limitaciones. Como con lock-and-key. AP es susceptible a ataques del tipo Spoofing. Después de la autenticación se inspecciona el tráfico subsiguiente del usuario, examinando la dirección IP origen del destino. Por lo tanto, si un hacker sabe que un usuario ha sido autenticado con éxito, el hacker puede comprometer al Router ejecutando algún tipo de ataque Spoofing, tomando ventaja de este conocimiento.

Otras limitaciones que AP incluye:

AP trabaja solamente para el tráfico que viaja internamente y no trabaja en el tráfico que pasa por el Router.

La autenticación debería ocurrir con HTTP, HTTPS, TELNET o FTP. Estos son los protocolos comúnmente más usados que proveen un mecanismo para la comunicación en dos direcciones, el cual es por que se ve solo estos cuatro métodos para la autenticación en el Router. Sin embargo, después de ser autenticada, basándose en cualquier descarga ACL's, el usuario puede acceder a otros recursos en la Red.

Con HTTP, la IOS de Cisco examina solamente las conexiones del puerto 80.

Si dos usuarios están compartiendo el mismo dispositivo, AP autentica solo al primer usuario, no al segundo, porque AP examina la dirección IP origen en paquetes para determinar si la autenticación ha sido realizada.

Puede realizarse la autenticación sin Java Script pero no es recomendable porque este no es seguro.

4.8.7 CONFIGURACIÓN AP

Para poder configurar AP se debe tomar en cuenta lo siguiente:
AP usa AAA para realizar autenticación y autorización.

- Está altamente recomendado que se use CBAC y ACL's para complementar AP.

Con HTTP y HTTPS autenticados, Cisco recomienda que se use Internet Explorer de Microsoft y Netscape Navigator en sus versiones actualizadas. Otros buscadores Web podrían o no trabajar.

Cuando se han resuelto los requisitos previos, se esta listo para proceder a configurar AP. Se necesitan configurar los siguientes componentes:
- Configuración de AAA en el Router.
- Configuración de AAA en el Server AAA.
- Preparación para HTTP Y HTTPS (FTP y Telnet no requieren configuración especial para AP).
- Configuración de políticas AP.
- Adaptación de AP
- Protección contra ataques de acceso.

(Ver demostración de configuración de técnica en cd-anexo: video #13: AP)

4.8.8 AAA (AUTENTICACIÓN, AUTORIZACION, CONTEO)

Se basa en una lista de permisos mediante el cual se puede administrar cuentas en el Router; todo con el fin de autenticar y autorizar requisitos. Para ello se requiere un Servidor AAA, el cual responde a las siguientes acciones:

- Asegurar acceso al Router
- Administrar Autenticación
- Autorizar comandos que se pueden ejecutar

- Mantener un control detallado de las acciones, en cuanto a conteo se refiere

4.8.8.1 AUTENTICACIÓN

Método para identificar usuarios, el cual incluye nombres de usuario para el acceso a determinado sitio.

4.8.8.2 AUTORIZACIÓN

Es usada para restringir las acciones que un usuario puede en determinado momento ejecutar o también para restringir los diversos servicios a los cuales puede acceder.

4.8.8.3 CONTEO

Mantiene un listado histórico de eventos de Autenticaciónes y Acciones de Autorización. Mantiene y genera logs de eventos. Una restricción de este componente es que requiere un servidor de seguridad externo para almacenar el historial del conteo actual.

4.8.8.4 BENEFICIOS DE AAA

- Escalabilidad
- Redundancia a través de múltiples servidores AAA
- Flexibilidad

Cuando se decide usar un servidor AAA para centralizar las políticas de seguridad, se hace necesario utilizar un protocolo de seguridad entre el Router y el servidor AAA; cabe mencionar que el protocolo es utilizado para intercambiar mensajes.

En la mayoría de situaciónes se usan protocolos de seguridad tales como:

- Kerberos.
- Terminal Access Controler Control System (TACACS+)

- Remote Authentication Dial-In User Service (RADIUS)

4.8.8.5 TACACS

Terminal de Control de Acceso-Sistema (TACACS), es el método que se utiliza para realizar las funciones de regulación y autenticación de las entradas por medio de conexiones remotas, el cual es su función principal aunque también puede autenticar servicios comunes en redes de área local.

Conocido por la facilidad de implementación, es adaptable y económico.
El Destacamento de Ingeniería de Internet (IETF) califica a TACACS como un Servidor de Autenticación, Autorización y Cuentas de Usuario (AAA).
El protocolo TACACS ha sido transformado dos veces, la primera versión utilizaba el protocolo UDP para transportar los datos, lo cual es inseguro y limitado en cuanto a sus capacidades. El protocolo que fue utilizado sobre UDP fue cambiando al más confiable TCP renombrando al protocolo XTACACS (TACACS extendido).

Cisco System adoptó TACACS y creo una implementación propietaria llamada TACACS+ para su arquitectura AAA. Las mejoras fueron hechas para separar las funciones de autenticación, autorización y cuentas de Usuario, resultando un producto más seguro que permite la encripción a servidores de acceso remoto. Además permite longitudes arbitrarias en los paquetes y el intercambio de parámetros de la autenticación, ya que la nueva versión es muy diferente a la origina; por lo tanto el estándar actual de la IETF para TACACS es TACAC+.

Para obtener acceso a un enrutador o servidores de acceso a red, TACACS provee una validación centralizada de los usuarios. Y puede ejecutarse en cualquier sistema operativo conocido especialmente los basados en Unix y Windows NT

Este protocolo usado para intercambiar información con el servidor de acceso a la red, intercambia información entre una base de datos centralizada y el dispositivo de red; este protocolo permite separar los servidores tanto de autenticación como de

autorización además permite el manejo de las cuentas de usuario lo cual hace más funcional y liviano al estar menos centralizado.

El servidor TACACS+ puede controlar las opciónes del servidor, definir usuarios y controlar la sección de autenticación. Se puede especificar a través de la opción de Sección de Operación de los parámetros de servicio, el nombre de archivo de las cuentas y las claves secretas. Una serie de usuarios y definiciones del archivo es el que retoma el archivo. El formato utilizado es: user = nombre de usuario o group = user name, seguido por un único par valor – atributo dentro de corchetes.

4.8.8.5.1 AUTENTICACIÓN

Hay tres tipos de autenticación TACACS: Inicio, Contestar y continuar. La descripción de los tipos de autenticación viene del paquete de inicio, el cual comienza cuando el cliente inicia la autenticación.
Con autenticación simple el paquete incluirá además el usuario y contraseña; el siguiente paso será la contestación. El servidor contesta al cliente con un paquete si el cliente requiere información adicional, ésta es pasada con un cliente contínuo y un servidor de contestación de paquetes.

La autenticación TACACS+ puede entrar cuando una conexión inicial en juego en la máquina o cuando un servicio que ha sido solicitado ha sido enviado y requiere privilegios especiales de acceso.
La conexión comienza cuando TACACS obtiene la información del usuario y la contraseña, la información es entonces encriptada usando MD5. Este paquete es transferido vía TACACS+ hacia el servidor, después de que el servidor recibe ese paquete se procede al proceso de autenticación. El servidor notifica al cliente donde es que la autenticación se ha hado ya sea si el cliente ha sido aceptado o denegado. A menos que la autenticación sea aceptada o denegada, el desafío-respuesta continuará, cuando una petición para servicio privilegiado o restringido es enviada, más información es solicitada por TACACS+ para poder procesar esta solicitud.

4.8.8.6 RADIUS (REMOTE AUTHENTICATION DIAL-IN USER SERVICE)

RADIUS (Servicio de Usuario de Acceso para Autenticación Remota) es un protocolo extensamente usado en ambientes de red. Comúnmente usado en ambientes de red. Comúnmente es usado por dispositivos de red como: servidores, enrutadores, switches, etc. Esto es usado por varios motivos:

Los sistemas generalmente no pueden ocuparse de un número grande de usuarios con la información distinta de autenticación. Esto requiere más almacenaje del que muchos sistemas poseen. RADIUS facilita la administración de usuarios centralizada.

Proporciona algún nivel de protección contra ataques externos y rastreos de información. Otros protocolos de autenticación proporcionan ya sea protección intermitente, protección inadecuada o protección inexistente.

La competencia primaria de RADIUS para la autenticación Remota es TACACS+ y LDAP.

4.8.8.6.1 FORMA DE APLICACIÓN

Según el modo de autenticación usada, las debilidades de usuario-contraseña pueden o no comprender la seguridad del esquema de autenticación subyacente. El tipo más común de intercambio: Una petición de acceso que implíca un nombre de usuario y contraseña de usuario, seguida por un acceso de aceptado, acceso denegado o un fracaso. El servidor en este caso es la entidad que tiene el acceso a una base de datos de información de autenticación que se puede usar para validar la petición de autenticación del cliente.

RADIUS es usado específicamente para las siguientes situaciónes:

- Si tienes múltiples dispositivos de seguridad y necesitas un protocolo para comunicarlos.

- Para implementar conteo de recursos, como mantener historial de cuanto un usuario se conecto y mantuvo en la red.
- Algunas cartas inteligentes soportan sistemas de autenticación solo RADIUS.
- Para usar PRE - autenticación antes de permitir el acceso de un usuario inicial para acceder a un dispositivo.

4.8.8.7 COMPARACIÓN ENTRE TACACS+ Y RADIUS

ÍTEM	TACACS+	RADIUS	COMPARACION
Conexión	TCP	UDP	UDP tiene menos over head, sin embargo, con TCP TACACS+ puede detectar mucho mas rápido una falla en el servidor y conmutar un backup. TCP puede hacer esto teniendo el Router en busca de una RST (closed connection) mensajes o usando tcp keepalives.
Encriptado	Payload	Password	TACACS+ es mucho mas seguro para encriptar el Payload entero, el cual incluye todos los usuarios e información de mensajes AAA. RADIUS encripta solo password, incluyendo nombres de usuarios y otra información de la cuenta son enviados en texto claro.
Autenticación y autorización	Separate	Combined	RADIUS combina funciones de autenticación y autorización, el cual significa que debería usar el mismo servidor o grupo para estas funciones. TACACS+ los separa, brinda mas control sobre el servidor que enlaza esta funciones.

Tabla 4.5-A Comparación entre TACACS+ y RADIUS

Protocolos WAN	PPP, ARAP, NetBIOS, NASI y X.25 PAD	PPP y SLIP	TACACS+ esta mucho mejor situado para situaciónes que involucran múltiples. Protocolos DIALUP, RADIUS soporta solo PPP y SLIP.
Router Command Authorization	Yes	No	TACACS+ te habilita el control de que comandos un usuario autenticado puede ejecutar en un ROUTER; RADIUS no lo hace.
Accounting	Basic	Advanc e	La mayor ventaja que RADIUS tiene sobre TACACS+ es el robust accounting, lo cual es porque muchos ISP usando monitoreo en las conexiones PPP.

Tabla 4.5-B Comparación entre TACACS+ y RADIUS

4.9 TCP / INTERCEPT TCP SYNFLOOD PREVENTING [3]

Una opción para tratar con ataques TCP SYN FLOOD, es implementar características de la IOS CISCO TCP INTERCEPT, la cual permite ocuparse de ataques DoS que intentan tomar ventaja de las debilidades en la manera que TCP establece conexión en una sesión de tres vías “three-way handshake”. TCP Intercept limita la eficacia de un ataque de TCP SYN flood que pudiera ocasionar un atacante.

4.9.1 TCP SYN FLOOD ATTACKS O ATAQUES DE INUNDACIÓN

Es un ataque fácil de iniciar. El atacante envía un flujo de segmentos TCP SYN con la intención de no terminar la comunicación de tres vías “tree – way handshake” para cada una de las conexiones. Típicamente el hacker combina esto con un ataque spoofing IP en el que paquete en la dirección origen se invalida en la dirección de

alguien más. Porque esta dirección no puede ser alcanzada (o si son direcciones de alguien más no son respondidas).
Esta situación genera que el servidor espere hasta que el tiempo que TCP maneja expire para la conexión, antes de remover la conexión de su tabla local de conexión. Esto ocasiona problemas porque utiliza recursos sobre el servidor TCP ocasionando con esto que se denieguen conexiones legítimas de TCP.

4.9.2 MODOS TCP INTERCEPT

TCP Intercept es una característica de la IOS Cisco que se utiliza para proteger servicios TCP contra ataques de flujo TCP SYN. TCP soporta dos modos de protección:

- Modo de Intercepción
- Modo de Reloj

4.9.2.1 MODO DE INTERCEPCIÓN

El modo de intercepción toma un acercamiento proactivo para los ataques de flujo TCP SYN. En modo Intercept, el Router intercepta todas las solicitudes de conexión TCP. Para el caso, el Router intercepta una petición y finge ser el servidor interno ocasionando con esto que se termine la conexión que un usuario externo desee establecer.

Una limitación del Modo Intercept es que no existe ninguna opción TCP que negocie entre el usuario externo y el Router (los cuales normalmente son los dispositivos en los que termina el servidor). Esto es porque el router no sabe de éstas opciónes de negociación hasta que el saludo de tres vías termina con el usuario externo y el Router comienza el segundo saludo de tres vías con el servidor interno de TCP. Típicamente esto no es un problema ya que TCP permite la negociación dinámica de éstos parámetros durante la operación normal de la sesión.

4.9.2.2 MODO WATCH (MODO RELOJ)

Mientras que el modo de intercepción toma un acercamiento proactivo para ocuparse de los ataques de inundación con TCP SYN, el modo “Watch” toma un acercamiento reactivo. Una de las ventajas principales del modo de intercepción es que remueve la carga de procesamiento de las inundaciones TCP SYN del servidor interno.
Sin embargo, esta es una espada de doble filo porque en la mayoría de los periodos una inundación de TCP SYN no esta ocurriendo, pero el Router todavía esta ejecutando el proceso de Intercepción, provocando una carga pesada en el Router.

Para solucionar este problema, puede usarse TCP Intercept en modo “Watch”, ya que toma un modo pasivo o reactivo, para acercarse a los ataques de inundación del TCP SYN. En el modo “Watch”, el Router mira pasivo la disposición de las conexiones TCP de usuarios a servidores. Este monitorea las conexiones y compara el valor a un valor del time out pre configurado (el cual por default es de 30 segundos). Si una conexión TCP no completa el saludo de tres vías en este periodo, la IOS Cisco envía un reset del TCP al Servidor para quitar la conexión. Para un ataque que esta directamente a un Servidor interno usando TCP, este remueve las conexiones “half-open”, así reduce la carga en el servidor y permite las conexiones legítimas que se procura sean procesadas.

4.9.3 TCP INTERCEPT, CONFIGURACIÓN Y VERIFICACIÓN

Habilitar TCP Intercept en el router requiere de un proceso simple. Solo un comando es requerido, pero típicamente se deberán contemplar ciertos parámetros para asegurar que las funciones de TCP Intercept están debidamente configuradas.

Al permitir TCP Intercept, el primer paso en la configuración de TCP Intercept es especificar cuáles sesiones TCP deben ser interceptadas en el Modo de Intercepción (Intercept Mode) o cuáles sesiones deber ser monitoreadas en el Modo de Reloj (Watch Mode).
Lo anterior se realiza mediante el uso del siguiente comando:

- Router(config)# ip tcp intercept list extended_ACL_#

En cuanto a la configuración, existen ciertos aspectos importantes los cuales deben precisarse en cuanto a los requerimientos del comando “TCP intercept”.

- Primero, este comando activa TCP Intercept. Nótese que el comando es ejecutado en el modo de configuración global y no en el modo de configuración de interfase.

- Segundo, se necesita haber configurado una ACL para especificar cuál tráfico será examinado por TCP Intercept.

Cuando se configura TCP Intercept, debe utilizarse para tratar Ataques de Inundación TCP proveniente de usuarios externos a la red. Esto se logra configurando Listas de Acceso Extendidas específicamente para TCP Intercept, logrando con ello filtrar el tráfico que debe ser monitoreado.

TCP Intercept utiliza contadores los cuales se pueden ajustar a las necesidades; estos son:

- Contador de tiempo embrionario

- Contador de tiempo de reinicio
- Contador de tiempo de conexión lenta.

Los contadores pueden ser configurados con los comandos siguientes:

Router (config) # ip tcp intercept watch-timeout seconds
Router (config) # ip tcp intercept finrst-timeout seconds
Router(config)# ip tcp intercept connection-timeout seconds

Además de los Modos de Intercepción y Reloj, TCP Intercept usa valores de umbral para ocuparse de un número excesivo de conexiones TCP durante un ataque de Inundación TCP SYN. TCP Intercept soporta dos umbrales: el primero basado en un número total de conexiones embriónicas, y el segundo basado en el número de peticiones de conexión durante el período de 1 minuto. Estos valores de umbrales pueden ser modificados.

Durante el tiempo de un ataque en el cual el router recibe un excesivo número de conexiones y uno de los dos umbrales es alcanzado, el router comienza a botar las conexiones embrionarias más antiguas. En el modo de Intercepción, el router reduce el tiempo de descanso de retransmisión para segmentos. En el modo de Reloj, el router reduce el tiempo automáticamente a la mitad del valor configurado.

4.10 RATE LIMITING (LIMITACIÓN - RANGO DE TARIFA) [3]

Con algunos tipos de ataques DoS no hay mucho que se pueda hacer para detener el flujo del ataques, especialmente en un ataque Distribuido DDoS en el cual el hacker realiza un Spoofing a la dirección origen utilizando la compañía que proporciona el servicio de Internet cómo causante del ataque. Rastrear estos tipos de ataques puede ser muy difícil.

En estas situación, la primera preocupación a resolver debe ser limitar el impacto del ataque en la red, lo cual puede ser realizado haciendo uso de Rate Limiting, ya que permite la habilitación de un ancho de banda restringido para una categoría de tráfico específica, tal como: ICMP, UDP o tipos de conexiones específicas.

Se plantean tres soluciones para Rate Limiting:
Commited Access Rate (CAR)
Class-Based Policing (CBP)
Application Recognition (NBAR)

Rate Limiting se utiliza mucho mejor en el Router del ISP que esta conectado a la Red. En otras palabras, si se esta experimentando un ataque de flujo que esta saturando el enlace a Internet, implementando Rate Limiting en el perímetro del Router, no funcionará muy bien.
Rate Limiting es una técnica que se configura para restringir la suma del tráfico de salida. Como ejemplo, si se es el reflector en un ataques Smurf, se puede usar Rate Limiting como solución temporal para limitar el flujo del tráfico que se esta enviando a la Red de una víctima.

4.10.1 ICMP RATE LIMITING

Muchos ataques del tipo DoS envían una inundación de tráfico a un dispositivo o dispositivos que no existen, causando una intervención en el Router para que conteste de regreso con un mensaje inalcanzable ICMP para cada destino desconocido. Un buen ejemplo de esta situación es un ataque del gusano, por ejemplo: el gusano SQL Slammer. Con este proceso, el gusano inadvertidamente trata de encontrar otra máquina con la misma debilidad. Esto usualmente lo hace con un barrido de ping. La mayoría de gusanos no son inteligentes en la manera como lo hacen de la siguiente manera: continuamente escanean las mismas redes, tratando de encontrar el mismo agujero o agujeros de seguridad que el gusano usa inicialmente para derribar uno de los dispositivos utilizados en la red.

(Ver demostración de configuración de técnica en cd-anexo: video #9: Rate Limit)

4.11 REVERSE PATH FORWARDING (REENVIO DE TRAYECTORIA REVERSA) [3]

Una herramienta útil de IOS Cisco para la prevención de Spoofing de direcciones IP es la utilización de RPF, que puede utilizarse para el tráfico multicast y unicast. Con RPF la IOS Cisco comprueba su tabla de enrutamiento para determinar si se acepta un paquete o se descarta.

RPF previene el Spoofing examinando la dirección IP origen en el paquete, la interfaz, el paquete que fue recibido y la información de enrutamiento en la tabla de ruteo. Si hay una contradicción, por ejemplo; la dirección origen no situada en la interfaz donde el Router piensa que el paquete pertenece (basándose en la tabla de ruteo) el Router descarta el paquete, hay que recordar que este tipo de spoofing es común en muchas formas de ataques DoS, como en los ataques Smurf. Unicast RPF remite solamente las direcciones IP origen válidas basado en información encontrada en la tabla de enrutamiento del Router este tipo de política de aplicación es común en IPS.

4.11.1 USO DE RPF

RPF trabaja mejor en el perímetro de la red, si se está usando dentro de la red se recomienda que se utilice mejor cuando el Router tiene mas Router específicos. Con sumarización de Ruta, un ataque Spoofing podría estar en proceso y este podría ser difícil para determinar desde que parte de la sumarización de la ruta esta ocurriendo el ataque.

Para amenazas externas, la mayoría de ISP's y compañías usan RPF, es probable que la mayoría sean ataques spoofing los cuales pueden ser una cara del pasado. Sin embargo, la mayoría de las conexiones POP (Punto de Presencias) que un ISP tiene lo mas difícil es convertirse para usar RPF porque podrían existir múltiples caminos para el origen. Usando RPF como fin para los posibles destinos de las direcciones es la mejor solución para que los ISP's conecten directamente a sus clientes.

RPF es mejor desplegado en el perímetro del Router en redes que tienen una conexión simple para el mundo de fuera. Seguramente, RPF trabaja en ambientes de conexión múltiple, como con Routers internos, pero esto podría no proveer la solución optima en detección de paquetes Spoofed.

Para que RPF funcione, CEF debe permitirse en el router. Esto es porque el router utiliza la base de Información de Trayectoria (FIB) de CEF para mejorar el proceso de las operaciones de búsqueda, la cual es construida de la tabla de ruteo del router. Es decir que RPF realmente no mira la tabla de ruteo del router; en lugar de ello, utiliza CEF FIB para determinar el ataque Spoofing.

4.11.2 LIMITACIONES DE RPF

A pesar de sus ventajas y utilidad en la detección y la prevención de ataques Spoofing, RPF tiene las siguientes limitaciones:

- RPF requiere la función CEF. Aquellos Routers que no suporten la función CEF no pueden hacer uso de RPF.
- La tabla de enrutamiento utilizan rutas asimétricas para el envío de tráfico a y desde un destino determinado. En esta situación se utilizan diversas trayectorias, lo cual crea problemas con el RPF ya que genera falsas alarmas de ataques Spoofing. Por lo tanto una sola conexión hacia Internet en el router es la situación ideal para utilizar RPF.

- Típicamente RPF no funciona bien cuanto está activado en interfaces internas del router, debido a ediciones asimétricas de ruteo.

4.11.3 CONFIGURACIÓN DE RPF

Antes de configurar RPF, debe asegurarse de haber realizado lo siguiente:

- Configurar filtro de salida: Permita solamente las direcciones que tenga asignadas o permita y deniegue todo lo demás. Al utilizar RPF, use filtro de salida para definir las políticas de salida.

- Configurar filtro de entrada: Deniegue todo y permita solamente las conexiones a los recursos internos de manera específica. También examine las direcciones de anomalías como interfaces de “loopback”, direcciones RFC, direcciones de broadcast.

- Configurar RPF ACL para operar con enrutamiento asimétrico si se tiene conexión dual de Internet en un router y el tráfico que retorna, proviene de una red diferente.

(Ver demostración de configuración de técnica en cd-anexo: video #10: RPF)

4.12 TÉCNICAS DE FAILOVER [3]

4.12.1 TRASLADO DE DIRECCIONES Y REDUNDANCIA

Una de las preocupaciones en el diseño de una red es la redundancia. Al hablar de redundancia, nos referimos al hecho de que la red siga funcionando si una conexión falla. Cisco en sus IOS más recientes, proporciona dos métodos de redundancia para la conversión de direcciones:

- Redundancia con NAT estático, haciendo uso de HSRP (Hot Standby Router Protocol).
- Seguimiento de Estado en el Traslado de Direcciones y Failover

Cabe mencionar que el protocolo HSRP brinda una alta disponibilidad de red y cambios transparentes de topología de red. Crea un grupo de Routers de reserva inmediata con un Router principal que brinda servicios a todos los paquetes enviados a la dirección de reserva inmediata. El Router en para el caso nuestro sería monitoreado por otro Router y si fallará, el Router de reserva recibe la posición principal.

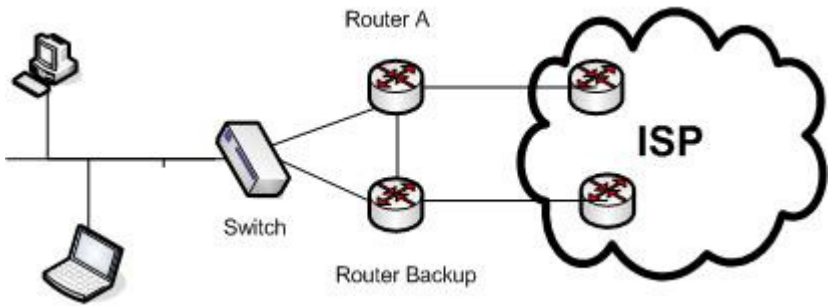


Figura 4.9 Ejemplo de conexión de failover (permite que al fallar el router principal el router de Backup entre en funcionamiento)

4.12.1.1 REDUNDANCIA CON TRASLADO DE DIRECCIONES ESTÁTICAS HACIENDO USO DE HSRP

Este método se utiliza típicamente en redes pequeñas, generalmente con una tan sola sub red, que está conectada a dos Routers para la redundancia. Para el caso, proporciona un constante funcionamiento en cuanto a conexión, ya que se proporciona el acceso a la red ante fallo de de las conexiones.
Tal es el caso de que en un diseño con un solo Router, si éste falla los usuarios externos a la red no podrían acceder a los recursos internos. Entonces para proporcionar redundancia es que se adiciona un segundo Router. Esto se logra haciendo uso de HSRP.

4.12.1.2 PROCESO DE LA REDUNDANCIA CON HSRP

Al usar HSRP para proporcionar redundancia en el traslado de direcciones estáticas (Static NAT), la configuración NAT se refleja en los dos Routers que se estén utilizando; tomando en cuenta que el Router principal es quién procesa todo el tráfico. HSRP es configurado en el Gateway por defecto; teniendo uno de los Router como Activo o Primario y el otro como Reserva y en espera. Se elige una IP virtual, la cual es asignada a los routers; esta IP virtual sirve para que los usuarios envíen el tráfico hacia un destino, en este caso al Router activo. El otro router monitorea al router primario y si éste falla inmediatamente pasa a la función de procesar el tráfico.

Nótese que solo NAT estático es considerado en este tipo de configuración; no NAT dinámico. Por lo tanto cualquier comando que configure en el Router Activo, deberá ser configurado en el Router que está en espera o de reserva.

HSRP es muy flexible ya que permite al administrador de la red controlar el comportamiento de los routers. La presencia de dos o más routers que pueden actuar como Gateway predeterminados en el mismo segmento de LAN es la primera parte de los criterios.
La configuración básica requiere como parámetro la dirección IP que se utiliza como dirección virtual del gateway predeterminado. Y se aplica a todos los routers que participen en el mismo segmento.

Para controlar cuál es el router de reenvío principal, se utiliza el comando de configuración de interfaz de IOS "*standby priority*". El comando adopta como parámetro un valor entre 0 y 255. El router del grupo HSRP que tenga la prioridad más alta se convierte en el router de reenvío.
El comando de interfaz de IOS "*standby preempt*" hace que el Router Principal reanude la función de envío a partir de otro router con prioridad más baja.

En algunas situaciónes, el estado operacional de una interfaz afecta directamente al Router Activo. Esto ocurre en particular cuando cada uno de los routers del grupo HSRP tiene una ruta de acceso distinta a otras partes de la red. Para ello la IOS ofrece la posibilidad de que el router pueda ajustarse; esta funcionalidad recibe el nombre de seguimiento de interfaces y se activa con el comando "*standby track*".

El funcionamiento de HSRP puede verificarse con el comando "*show standby*".
El comando adopta como parámetro opcional la interfaz específica en la que se va ha mostrar la información de HSRP. Sin dicho parámetro la información de HSRP aparece en todas las interfaces.

El comando "*show standby"* muestra la información de HSRP, que incluye el estado de los reenvíos, la prioridad HSRP y las interfaces, en las cuales se realizan seguimientos del router y consultas. También muestra información acerca de la dirección IP de reserva configurada y las direcciones IP de los posibles routers de reserva de cada grupo HSRP.

Una de las desventajas del HSRP original era que no permitía al administrador de red compartir la carga del tráfico que cruza ambos routers del grupo de reserva. Básicamente, el router de reserva estaría inactivo a menos que fallará el router activo.
Para solucionar este problema, se añadió al software IOS la capacidad para admitir varios grupos HSRP en la misma interfaz. En la misma interfaz se pueden crear varios grupos HSRP, cada uno de ellos con una dirección IP virtual distinta, para respaldarse unos a otros. Con dos grupos HSRP y dos direcciones IP virtuales

definidas, el administrador de red puede configurar el Gateway predeterminado en algunos de los host con una de las direcciones virtuales de HSRP, y en los host restantes, con la otra. Aunque no consigue un equilibrado de la carga exactamente igual, esta configuración comparte la carga entre los dos routers en lugar de sobrecargar sustancialmente uno de ellos mientras el otro se queda completamente inactivo.

Mediante la especificación de un número de grupo en todos los comandos "*standby"*, se pueden crear varios grupos HSRP. Por ejemplo, "*standby 1 ip address* [dirección IP]" y "*standby 1 priority 100"* especifican que estos comando HSRP se aplican al grupo de reserva 1. Los comandos "*standby 2 ip address* [dirección IP]" y "*standby 2 priority 100"* especifican que estos comando HSRP se aplican al grupo de reserva 2.

Para configurar NAT con HSRP, se debe seguir los siguientes pasos:

- Paso 1: Configurar HSRP
- Paso 2: Integrar la configuración de NAT estático con HSRP

Para configurar HSRP se utilizan los siguientes comandos:

Router (config) # interface type [slot_#/]port_#

Router(config-if)# ip address IP_address subnet_mask *(1)*

Router(config-if)# no ip redirects *(2)*

Router(config-if)# standby [group_#] name [HSRP_group_name] *(3)*

Router(config-if)# standby [HSRP_group_#] ip IP_address *(4)*

Router(config-if)# standby [group_#] preempt

Router(config-if)# standby [group_#] priority priority_#

Router(config-if)# standby [group_#] track interface decrement_value

Los únicos comandos básicos de interfaces requeridos están marcados con los números al lado derecho, los dos últimos son opciónales.

Luego de configurado el HSRP, podemos configurar NAT con los siguientes comandos:

Router(config)# ip nat inside | outside source static local_IP_address global_IP_address redundancy HSRP_group_name

Router(config)# interface type [slot_#/]port_#

Router(config-if)# ip nat {inside | outside}

La principal diferencia con la configuración del NAT estático es la adición de los parámetros de redundancia. El nombre del grupo del HSRP especificado es que debe coincidir la configuración con el nombre del comando "*standby".*

Después de haber configurado NAT estático con el HSRP, se puede utilizar standby (estado de espera). Para verificar esta característica esta disponible el siguiente comando "*show ip nat translations verbose".*

Seguimiento de Estado en el Traslado de Direcciones y Failover (SNAT Failover)

El principal problema de Redundancia con NAT estático, haciendo uso de HSRP es que no lleva un seguimiento de estado en el traslado de direcciones. Ya que provee Redundancia solo para traslado estático NAT. En otras palabras si se hace uso de traslado de direcciones dinámicas, todas éstas se perderían cuando el Router Activo o Primario falle; esto causaría problemas de conectividad.

4.12.2 CARACTERÍSTICAS Y RESTRICCIONES DE SNAT FAILOVER

En esta solución, en los Routers se efectúa dos traslados de direcciones, una primaria y una de respaldo. El router primario en el grupo, realiza el traslado de direcciones. El Router de respaldo recibe actualizaciónes de traslado de direcciones provenientes del router Primario y a la vez verifica que éste se encuentre Activo o en funcionamiento. Si el router primario falla, el router de respaldo comienza su funcionamiento utilizando la tabla de direcciones que fueron compartidas con el router primario.

SNAT puede trabajar haciendo uso de HSRP. Cabe mencionar que este proceso es diferente que el descrito anteriormente ya que con SNAT y HSRP la redundancia puede ser para traslados estáticos y para traslados dinámicos de direcciones.
SNAT no soporta información de empaquetamiento de direcciones. Por lo tanto aplicaciones como FTP, NetMeeting, RAS, Skinny, TFTP y routeo asimétrico no funcionan

4.12.3 SNAT CON HSRP

SNAT puede ser configurado de dos maneras: con HSRP y sin el.
Pasos para configurar el SNAT con HSRP:

- Paso 1: Configurar HSRP
- Paso 2: Configurar SNAT Failover
- Paso 3: Configurar el Traslado de Direcciones.

4.12.3.1 CONFIGURACIÓN DE HSRP CON SNAT FAILOVER

Router(config)# ip nat stateful id router_ID_#

Router(config-ipnat-snat)# redundancy HSRP_group_name

Router(config-ipnat-snat-red)# mapping-id mapping_ID_#

El comando *ip nat stateful id* especifica e identifica el Router en un determinado grupo SNAT. Cada Router participante tiene que tener un identificador único. El rango de este identificador puede estar entre 1 y 2,147,483,647. Por ejemplo si dos routers participan con SNAT Failover, puede utilizarse como identificadores 1 y 2 respectivamente. El comando *redundancy* especifica el nombre del grupo HSRP para la redundancia. El comando *mapping-id* especifica el número de identificación para el traslado que el router primario enviará a router en espera.
Cada Router del grupo necesita un identificador único, el nombre del grupo HSRP y el identificador de mapeo deben ser iguales.
(Ver en Anexo 3 página 228 para leer información de lo que se utiliza hoy en día)

4.12.4 CONFIGURAR EL TRASLADO DE DIRECCIONES

Después de haber configurado HSRP con SNAT Failover, procedemos a configurar el traslado de direcciones. Para traslados estáticos se debe configurar manualmente cada uno de los router involucrados en el grupo HSRP; aunque debe recordarse que SNAT Failover aplica solo para traslados dinámicos.
Para configurar el traslado dinámico de direcciones usar el primer comando y cualquiera de los siguientes según sea el caso:

Router(config)# ip nat pool global_pool_name begin_IP_address end_IP_address prefix-length prefix_length

Router(config)# ip nat inside source route-map route_map_name pool global_pool_name mapping-id mapping_ID_# [overload]

Router(config)# ip nat inside source list ACL_#_or_name pool global_pool_name mapping-id mapping_ID_# [overload]

El comando *ip nat pool* define las direcciones globales a utilizarse para el traslado de las direcciones locales.
Los 2 comandos siguientes especifican cuáles direcciones locales serán transformadas por las direcciones globales. Como parámetro adicional se tiene *mapping-id* el cual indica a la IOS que el traslado dinámico es un traslado SNAT. Posterior a esto se debe especificar cual interfase es interna y cual externa para que se lleve a cabo el traslado de direcciones; para ello se especifica mediante el comando *ip nat {inside | outside}.*

(Ver demostración de configuración de técnica en cd-anexo: video #12: Failover)

4.13 PLANTEAMIENTO DE SOLUCIÓN A IMPLEMENTAR

Es importante mencionar la importancia que se le da, al uso de una combinación de herramientas para lograr los objetivos que las Empresas se proponen, dado que hoy en día no basta con solo tener un Firewall y garantizar la seguridad en la red.

Por lo que se ha determinado y se propone que todas las pequeñas y medianas empresas deben tener una solución de seguridad en Internet.

Hoy en día, las soluciones de seguridad que se implementan en las entidades requieren varias capas de protección para los diversos tipos de amenazas que afrontan las redes en la actualidad, utilizando tanto hardware como software.

PLANTEAMIENTO

Ante las tentativas de ataques a la red en una organización, se considera como factor importante dentro de las entidades garantizar que los recursos informáticos estén disponibles para cumplir sus propósitos, es decir, que no esten dañados o alterados por circunstancias o factores externos.

Es importante tomar en cuenta, que en el mercado existe una variedad de productos, técnicas, herramientas (ya sean hardware o software) adicionando la definición de reglas técnicas y/o actividades destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible de robo, pérdida o daño, realizándose de manera personal, grupal o empresarial.

En base a la investigación realizada, se plantea como alternativa para salvaguardar proteger los recursos que en esta se encuentren: implementar el prototipo de firewall utilizando Router Cisco con IOS, que soporte características de Firewall, VPN e IDS.

Permitiendo a pequeñas y medianas empresas proveer un nivel optimo y confiable de seguridad en sus redes informáticas. Recomendando el planteamineto de políticas de seguridad acordes a las necesidades de las organizaciones, tomando en cuenta que estas pueden estar sujetas a cambios y deben acoplarse a las necesidades cambiantes de la entidad y de las necesidades que en ella surjan.

En este sentido se hace énfasis, como parte importante de un plan de seguridad limitar y restringuir el acceso a la información sensible de una empresa, es decir, a todos aquellos datos cuya pérdida puede afectar el buen funcionamiento de la organización.

En la siguiente tabla se presentan los ataques que el prototipo será capaz de detectar en la red, como parte del plan de seguridad a considerar:

ATAQUES POR CATEGORIA		
Ataques de rastreo	**Ataques de**	**Ataques de**

de tráfico	Negación de servicio (DoS)	Acceso no autorizado (Spoofing)
Ethereal	SMURF	Spoofing-Looping
EffeTechHTTPSniffer	Fraggle Attack	Spoofing
Sniffer	TCP SYN flood Attacks	DNS Spoofing
Angry IP scanner	IP Flooding	Web Spoofing
SnoopAnalyzer Standard	Broadcast	IP Splicing-Hijacking
Netinfo	PING OF DEATH	Utilización de BackDoors
	IP Spoofing	Utilización de Exploits
		Obtención de Passwords
		Uso de Diccionarios

Tabla 4.6 Tipos de Ataques por categoría

Es importante tomar en consideración, que las amenazas no disminuirán y las vulnerabilidades no desaparecerán en su totalidad, por lo que los niveles de inversión en el área de seguridad en cualquier empresa, deberán ir acordes a la importancia de la información en riesgo.

Así mismo, cada dispositivo que conforma la red empresarial necesita un nivel de seguridad apropiado y la administración del riesgo implica una protección multidimensional (firewalls, autenticación, antivirus, controles, políticas, procedimientos, análisis de vulnerabilidad, entre otros) y no únicamente tecnología.

Por lo que a la vez, se propone una constante actualización y verificacion de parametros de seguridad en las redes informáticas, siendo necesario ante los cambios constantes en las tecnologías de información y lo vulnerable que esta se vuelve día con día, asi como las demandas por parte de los usuarios.

CAPÍTULO 5. DISEÑO DEL SOFTWARE

5.1 INTRODUCCIÓN

El objetivo del Software de Configuración y Monitoreo es el de proponer una herramienta para poder configurar Enrutadores con funciones de Firewall, así como también el poder monitorear ciertos eventos registrados por el Firewall.

5.2 PLANTEAMIENTO DEL PROBLEMA

A continuación se detallan las causas por los cuales se hace necesaria la creación del Software de Configuración y Monitoreo.
Necesidad de tener un entorno amigable para las diferentes configuraciones que se puedan realizar en un Router con Funciones de Firewall.

Actualmente son bastante limitadas las herramientas que permitan realizar configuraciones a los Router con funciones de Firewall y de manera gratuita.
La complejidad de los sistemas actuales para realizar las diversas configuraciones en los routers.

5.3 PLANIFICACIÓN DEL SOFTWARE

5.3.1 ÁMBITO DEL SOFTWARE

5.3.1.1 SISTEMA CONFIGURACIÓN Y MONITOREO

El sistema permitirá realizar lo siguiente: Configuraciones básicas del Router, Configuraciones del Router con Funciones de Firewall y Monitoreo de los eventos generados por el Router en Función de Firewall.
El sistema tendrá la opción de recibir ciertos parámetros para las diversas configuraciones que se quieran realizar en el router, tales como Nombres, contraseñas.

En cuanto al aspecto de rendimiento, el programa en sus diferentes funciones proporcionará un tiempo corto de respuesta a las configuraciones que se desean realizar en un router, buscando con ello minimizar los tiempos para determinada función.

Se hará uso de un servidor TFTP para mantener la sesión con el router que se desee configurar y monitorear.
Para la creación de las diferentes interfaces se ha propuesto un ambiente web en el cual se va a utilizar PHP. Para la creación de la base de datos se propone el uso de MySQL, buscando con ello satisfacer las demandas de los posibles usuarios en cuanto a no incurrir en gastos de licencias de software.

5.3.2 ESTIMACIÓN DE RECURSOS

5.3.2.1 RECURSOS HUMANOS

Dentro a lo que se refiere estimación de recursos uno de los aspectos importantes es la estimación de los recursos humanos. El cual consiste en el número de personas requeridas para realizar el desarrollo del sistema.
Para lograr esta estimación, hacemos uso de una estimación del esfuerzo de desarrollo (persona – mes), utilizando la técnica de estimación basada en el proceso, en el cual se definen cada una de las actividades o tareas que conforma nuestro proceso de desarrollo del sistema.
A continuación se muestran cada una de las actividades del proceso, también cabe mencionar que las estimaciones iniciales del esfuerzo se proporcionan para la comunicación con el cliente, planificación y análisis de riesgos**.**

5.4 PROCESOS

5.4.1 INICIO DE SESIÓN (IS)

El sistema permitirá realizar la sesión con el dispositivo que se desea configurar, en este caso iniciar sesión con un router. Para ello se establecerán parámetros que permitan la comunicación entre el router y el sistema de configuración de tal forma que los datos ingresados en el sistema de configuración sean reconocidos por el router.

5.4.2 REGISTRO DE USUARIO (RU)

Con la finalidad de ofrecer seguridad en el sistema al momento de realizar las diversas configuraciones en el router. El sistema deberá realizar un registro de usuario solicitando las contraseñas que le dan el privilegio para realizar cambios de configuración en el router.

5.4.3 AUTOMATIZACIÓN DE CONFIGURACIONES (AC)

Cuando el usuario alimente el sistema con cada uno de los requisitos de configuración, éste actualizará casi de manera automática la configuración en el router. Previo a esta operación el sistema dará la oportunidad de visualizar la nueva configuración para que el usuario acepte o deniegue dicha configuración.

5.4.4 INTERFACE DEL USUARIO Y FACILIDADES DE CONTROL (IUFC)

Esta actividad comprende diferentes interfaces necesarias para el funcionamiento del sistema, dentro de las cuales están:

Interfase del usuario para ingresar al sistema: en cuanto a la seguridad del sistema, buscando con ello la protección de las configuraciones. Para ello se diseñará un formulario propio para el ingreso al sistema de configuración mediante el cual se solicitará el respectivo usuario y la contraseña.

Interfase de Configuraciones Básicas y de Firewall: El sistema permitirá crear un archivo de configuración en una extensión específica, para el caso la extensión del archivo será "txt".

Una vez hecha la configuración, el sistema creará el archivo en una carpteta específica para que posteriormente sea enviado al router vía TFTP

Interfase de Monitoreo de eventos: éstas permitirán presentar en pantalla al usuario cifrás en cuanto a intrusiones que se han querido generar o en otras palabras la cantidad de ataques recibidos.

5.4.5 ELABORACIÓN DE REPORTES E INFORMES (ERI)

El sistema tendrá como opción adicional el poder generar un informe a nivel de pantalla mostrando cantidades y porcentajes de lo que se haya configurado en el router.

5.4.6 GESTIÓN DE LA BASE DE DATOS (GBD)

Se creará una base de datos que pueda dar soporte al sistema, tomando en cuenta tanto los flujos de datos como el diccionario de datos. En la base de datos se almacenarán cada una de las líneas de comando y además se llevará el registro de los eventos generados por el router con función de firewall.

En la tabla se presentan las indicaciones del esfuerzo estimado que se requiere para el análisis, diseño, codificación y prueba.

5.4.7 TABLA DE ESTIMACIÓN BASADA EN EL PROCESO

Actividad	**CC**	**Planificación**	**Análisis De Riesgos**	**Ingeniería**		**Construcción Entrega**		**EC**	**Totales**
Tarea				***Análisis***	***Diseño***	***Código***	***Prueba***		
Función									
IS				0.12	0.20	0.08	0.12		**0.52**
RU				0.12	0.20	0.12	0.12		**0.56**
AC				0.08	0.16	0.12	0.12		**0.48**
IUFC				0.16	0.16	0.08	0.16		**0.56**
ERI				0.08	0.16	0.12	0.12		**0.48**
GBD				0.10	0.15	0.15	0.10		**0.45**
Totales	**0.12**	**0.12**	**0.12**	**0.7**	**1.19**	**0.75**	**0.86**		**3.86**
% Esfuerzo	**3.11 %**	**3.11 %**	**3.11 %**	**18.13 %**	**30.82 %**	**19.43 %**	**22.27 %**		

CC = comunicación con el cliente EC = evaluación cliente

Tabla 5.1 Estimaciones basadas en procesos

Calculo de esfuerzo:

A continuación se presentan los datos correspondientes a los diferentes porcentajes de esfuerzo de cada función y la actividad del proceso de software.

Comunicación con el Cliente	0.12 / 3.86 * 100 % =	3.11 %
Planificación	0.12 / 3.86 * 100 % =	3.11 %
Análisis de Riesgos	0.12 / 3.86 * 100 % =	3.11 %
Análisis (Ing.)	0.7 / 3.86 * 100 % =	18.13 %
Diseño (Ing.)	1.19 / 3.86 * 100 % =	30.82 %
Código	0.75 / 3.86 * 100 % =	19.43 %
Prueba	0.86 / 3.86 * 100 % =	22.27 %

Tabla 5.2 Datos con los porcentajes de esfuerzo

Según la tabla de estimación basada en e proceso y el cálculo del esfuerzo, se puede observar que las estimaciones iniciales del esfuerzo se proporcionan para la *comunicación con el cliente, planificación y análisis de riesgos.* Los totales horizontales y verticales proporcionan una indicación del esfuerzo estimado que se requiere para el análisis, diseño, codificación y pruebas.

Se debe señalar que el 48.95 % de todo el esfuerzo se aplica en las tareas de ingeniería, indicando la importancia relativa de este trabajo.

Basado en una tarifa laboral de $ 375 por persona y en un período de “8” semanas, el costo total estimado del proyecto es de $ 4,500 y el esfuerzo estimado es de 3 personas – mes.

5.4.8 ANÁLISIS DEL SISTEMA

5.4.8.1 PARTICIÓN DEL PROBLEMA

A menudo se sabe que los problemas son demasiado grandes o complejos para comprenderlos totalmente. Por este motivo tendemos a hacer una partición o una división de los diferentes problemas en partes con el fin de que puedan entenderse fácilmente y establecer las interacciones entre las partes de manera que se pueda conseguir la función global.

A continuación se presenta la partición horizontal del problema; la cual viene siendo una representación de cómo puede ser solucionado el problema planteado en cuanto al desarrollo del sistema.

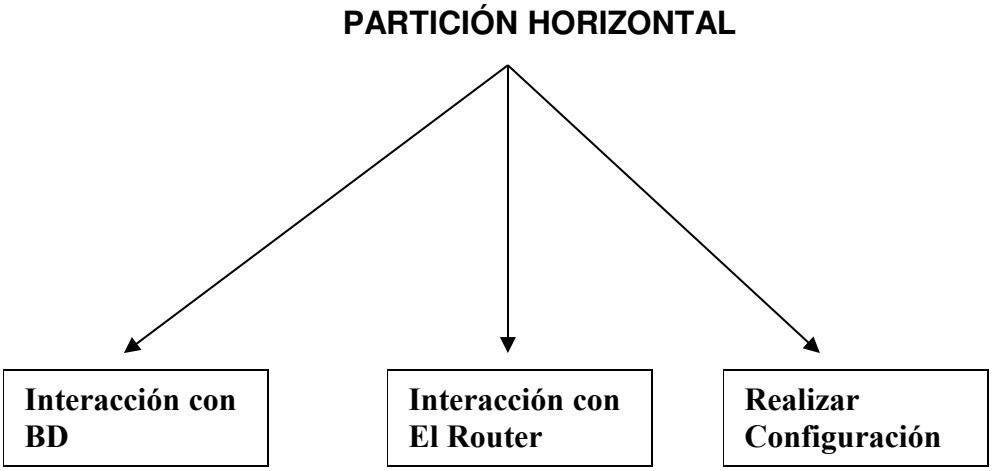


Figura 5.1 Etapas de la Partición Horizontal.

5.5 HERRAMIENTAS UTILIZADAS PARA EL DESARROLLO DEL SOFTWARE

5.5.1 SOFTWARE A UTILIZAR

PHP [19]

PHP (acrónimo de "PHP: Hypertext Preprocessor"), es un lenguaje interpretado de alto nivel en páginas HTML y ejecutado en el servidor.

Traduciendo la definición del FAQ de PHP.net: "El PHP es un lenguaje de script incrustado dentro del HTML. La mayor parte de su sintaxis ha sido tomada de C, Java y Perl con algunas características especificas de si mismo. La meta del lenguaje es permitir rápidamente a los desarrolladores la generación dinámica de páginas".

Una de sus características más potentes es su suporte para gran cantidad de bases de datos.

Entre su soporte pueden mencionarse InterBase, mSQL, MySQL, Oracle, Informix, PosgreSQL, entre otras.

PHP también ofrece la integración con las varias bibliotecas externas, que permiten que el desarrollador haga casi cualquier cosa desde generar documentos en pdf hasta analizar código XML.

PHP es la opción natural para los programadores en máquinas con Linux que ejecutan servidores Web con Apache, pero funciona igualmente bien en cualquier otra plataforma de UNIX o de Windows, con el software de Netscape o del Web Server de Microsoft. PHP también utiliza las sesiones de HTTP, conectividad de Java, expresiones regulares, LDAP, SNMP, IMAP, protocolos de COM (bajo Windows).

APACHE 1.3 [20]

Apache es un Servidor Web desarrollado por el grupo Apache.

Según estudios realizados por diferentes empresas el Servidor Web más utilizado en Internet es Apache.

Licencia bajo la que se distribuye Apache

Apache se distribuye bajo una licencia especial Apache Software License.

Los binarios y el código fuente de Apache se pueden usar y distribuir de forma libre y en las condiciones mencionadas en la licencia.

Plataformas para las que está disponible Apache

Apache está disponible para diversas plataformas:

- FreeBSD, NetBSD, OpenBSD

- GNU/Linux
- Mac OS y Mac OS X Server
- Netware
- OpenStep/Match
- UNIX comerciales como AIX (R), Digital UNIX (R), HP-UX (R),IRIX (R), SCO (R), Solaris (R), SunOS (R), UnixWare (R)
- Windows (R)

CARACTERÍSTICAS DE APACHE

Independencia de plataforma

Como ya hemos visto Apache funciona en casi todas las plataformas actuales. Debido a esto podemos escoger la plataforma que más se adapte a nuestras características, y también podemos cambiar de plataforma si en un momento determinado una plataforma nos ofrece más ventajas.

Gracias a esto se produce una independencia tecnológica del fabricante de hardware lo que hace que el fabricante esté en continua evolución y ofreciendo productos de calidad a sus clientes ya que en caso de disconformidad por parte de los clientes estos siempre podrían elegir otra plataforma.

Autenticación de diferentes tipos

Apache permite la autenticación de usuarios en varias formas.

Apache permite el uso de bases de datos DBM para la autenticación de usuarios. De esta forma se puede restringir el acceso a determinadas páginas de un sitio Web de una forma sencilla y de fácil mantenimiento.

Creación de contenidos dinámicos

- Apache permite la creación de sitios Web dinámicos mediante:
- El uso de CGI's.

- El uso de Server Side Includes (SSI).
- El uso de lenguajes de Scripting como PHP, javascript, Python.
- El uso de Java y páginas jsp.

Gestión de logs

Apache permite la creación de ficheros de log a medida del administrador.

Apache utiliza el formato Common Log Format (CLF) para la generación de los logs de error. Este formato es usado por varios Servidores Web y existen herramientas para el análisis de ficheros con este formato

Gran escalabilidad

Se pueden extender las características de Apache hasta donde nuestra imaginación y conocimientos lleguen.

Apache soporta Dinamic Shared Object (DSO). Gracias a ello se pueden construir módulos que le den nuevas funcionalidades que son cargadas en tiempos de ejecución.

Negociación de contenido

Apache puede facilitar información en varios formatos para que un determinado cliente pueda interpretarla.

MySQL [21]

MySQL Database Server es la base de datos de código fuente abierto más usada del mundo. Su ingeniosa arquitectura lo hace extremadamente rápida y fácil de

personalizar. La extensiva reutilización del código dentro del software y una aproximación minimalística para producir características funcionalmente ricas, ha dado lugar a un sistema de administración de la base de datos incomparable en velocidad, compactación, estabilidad y facilidad de despliegue. La exclusiva separación del Core Server del manejador de tablas, permite funcionar a MyQSL bajo control estricto de transacciones o con acceso a disco no transaccional.

MySQL es software de fuente abierta

Fuente abierta significa que es posible para cualquier persona usarlo y modificarlo. Cualquier persona puede bajar el código fuente de MySQL y usarlo sin pagar. Cualquier interesado puede estudiar el código fuente y ajustarlo a sus necesidades. MySQL usa el GPL (GNU General Public License) para definir que puede hacer y que no puede hacer con el software en diferentes situaciones. Si usted no se ajusta al GLP o requiere introducir código MySQL en aplicaciones comerciales, usted puede comprar una versión comercial licenciada.

¿Porqué usar MySQL Server?

MySQL Database Server es muy rápido, confiable y fácil de usar. Si eso es lo que usted está buscando, debe tenerlo y usarlo. MySQL Server también tiene un práctico set de características desarrollado en cercana cooperación con nuestros usuarios. Su conectividad, velocidad y seguridad hacen a MySQL altamente satisfactorio para acceder a bases de datos en Internet.

5.5.2 INTERCONEXIÓN DE TECNOLOGíAS UTILIZADAS

Relacionar la manera en que interactúan todas las tecnologías sobre las cuales se ha desarrollado el sistema y sobre las cuales se tiene que implementar: la base de datos (MySQL), diseño de la aplicación (PHP), servidor de conexión (Apache) servidor de desarrollo (Windows); es lo que se puede denominar interconexión de las tecnologías y se trata de enlazar la relación que tiene y la dependencia que parte de una de la otra, ya que es el conjunto como tal, lo que hace el funcionamiento correcto de toda la aplicación.

5.5.3 DESCRIPCIÓN DE DIAGRAMAS DE FLUJO

5.5.3.1 DIAGRAMA DE CONTEXTO

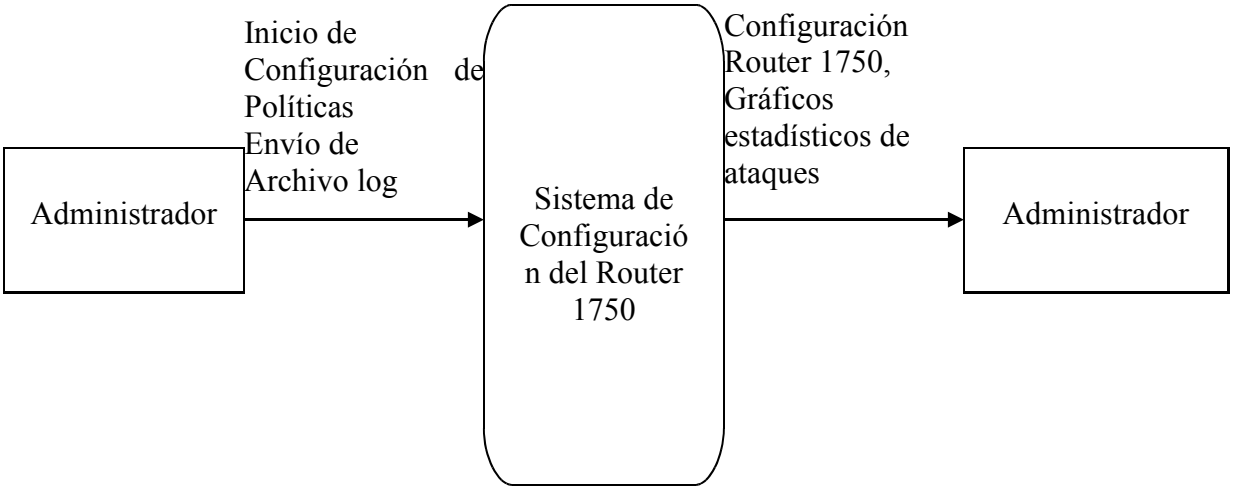


Figura 5.2 Diagrama de Contexto del Sistema

En el diagrama anterior se muestra la relación que existe entre el sistema de configuración del router y el administrador. El bloque central representa el proceso principal en donde el sistema realiza la configuración del router, además monitorear el tráfico para presentar posteriormente estadísticas.

Los terminadores que se encuentran están en relación al sistema debido a que son los administradores los únicos que poseen permiso para la configuración del router y ellos son los que utilizarán los resultados del monitoreo del tráfico que pasa por el router para la toma de alguna acción que permita mantener o incrementar la seguridad utilizando algunas de las técnicas mencionadas.

La configuración del router dependerá de las políticas establecidas con anterioridad y según los requerimientos de la oficina en donde se apliquen.

5.5.4 PROCESO DE CONFIGURACIÓN DE POLÍTICAS

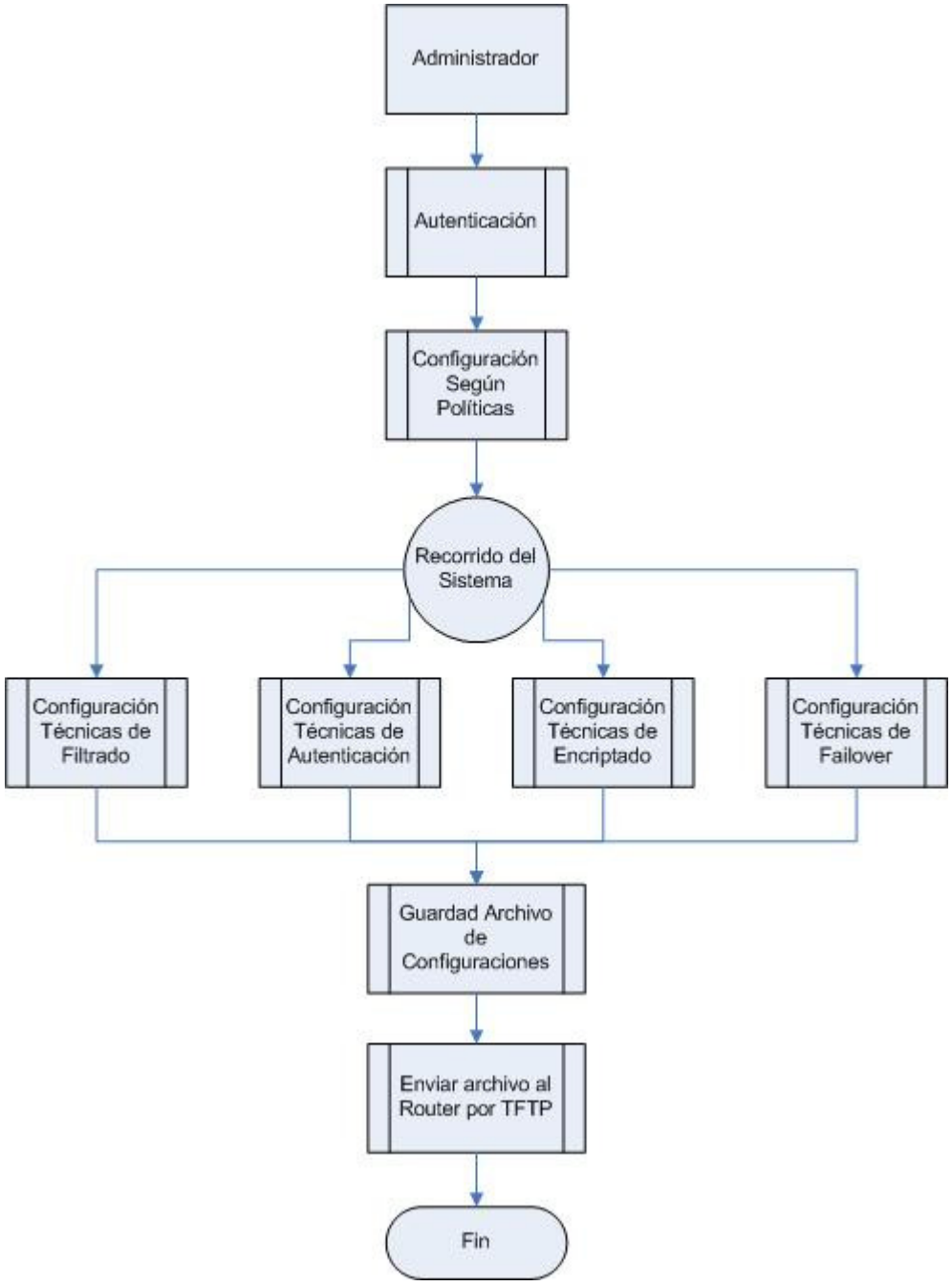


Figura 5.3 Diagrama de Configuración del Router con funcionalidad de Firewall utilizando técnicas de Filtrado, autenticación, encriptado y Failover

El administrador inicia la sesión para lo cual es validado con su usuario y contraseña, luego se inicia la configuración del router, que dependerá de las políticas que la empresa a establecido y técnicas de filtrado, autenticación, encriptado así como la técnica de failover. Finalmente se carga la configuración al router por tftp para que pueda usarse.

5.5.5 PROCESO DE CONFIGURACION DEL SISTEMA DE MONITOREO

Figura 5.4 Diagrama de proceso para monitorear de tráfico en el Router

Para que el router pueda capturar el tráfico que pasa en sus interfaces debe configurar para que cumpla esta función. Este tráfico es enviado a la Base de Datos de MySQL de la cual posteriormente se obtendrán las estadísticas del tráfico que pasa por las interfaces del router.

5.6 DISEÑO DE LA INTERFASE

Una de las finalidades principales que se buscan además de la funcionalidad del sistema, es la homogeneidad del mismo, lo cual permita a los diferentes usuarios el fácil manejo de la aplicación y el estar familiarizado con el ambiente web ya conocido.

A continuación se encuentran las principales interfaces del sistema, en donde se realizan las siguientes configuraciones:

- **Acceso al Sistema**

Interfaz inicial del sistema

Sirve para poder ingresar a la página de Bienvenida de configuración es necesario autenticarse por medio del usuario y la contraseña respectiva, información que es brindada por el usuario.

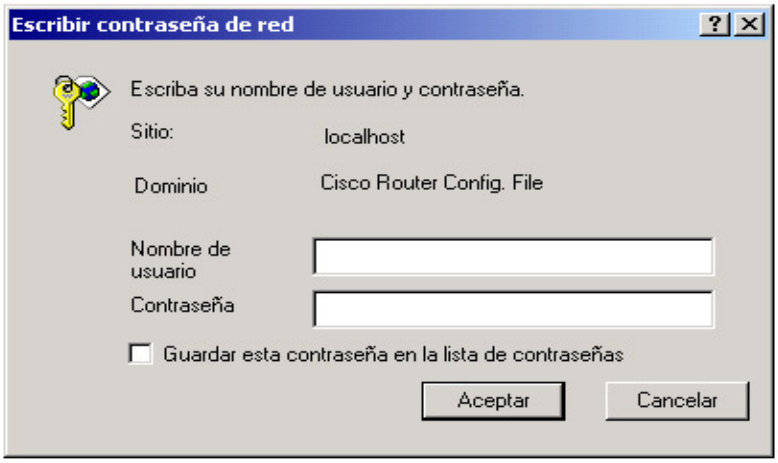


Figura 5.5 Seguridad estándar que permite el apache

Página de Bienvenida

La pantalla de inicio muestra un saludo de bienvenida y presenta un botón en javascritp que carga la primera página del proyecto.

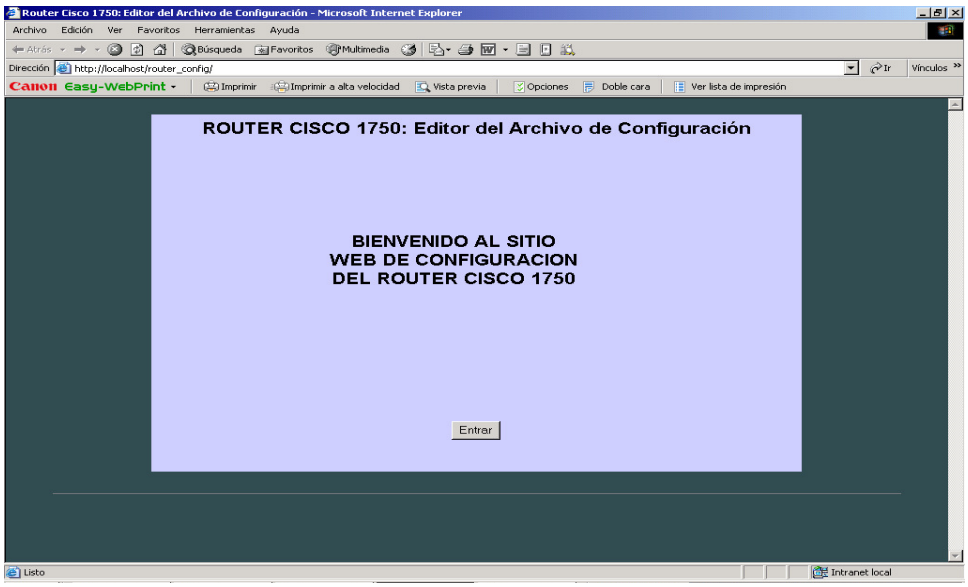


Figura 5.6 Página de Bienvenida al sistema de configuración del Router

Página de Configuración

En la página de configuración se realizan todas las configuraciones básicas del Router según las políticas establecidas. Las técnicas que se utilizan son: técnicas de filtrado, autenticación, ecriptado y técnicas de failover.

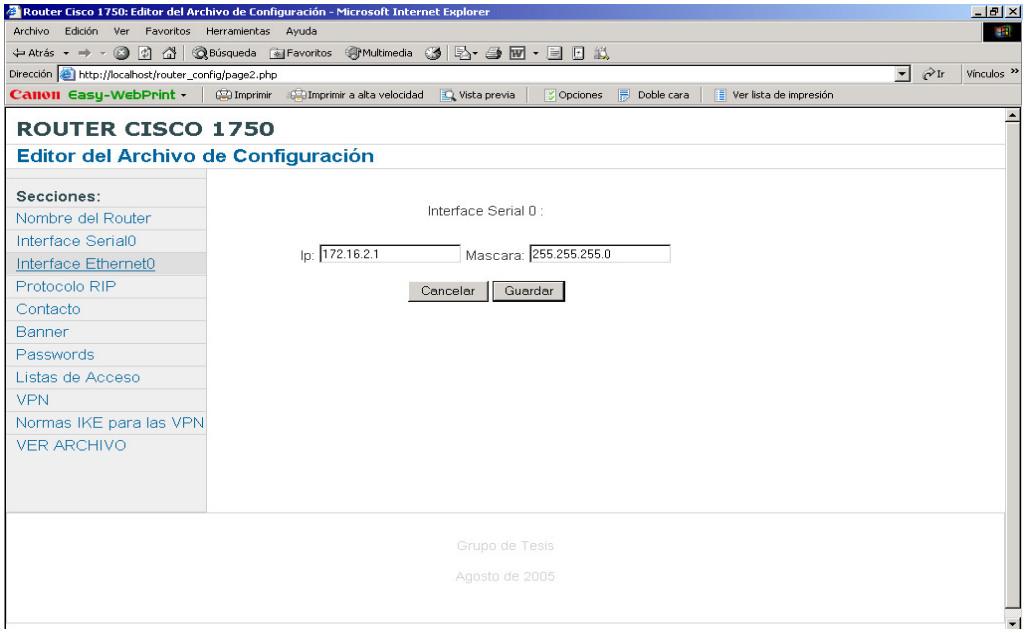


Figura 5.7 Página principal de configuración del router 1750

(Ver Anexo 6. Manual de usuario, página 302 de este documento)

5.6.1 REQUISITOS DE HARDWARE Y SOFTWARE

Administrador	
Requerimientos mínimos	**Requerimientos ideales**
Hardware	
Procesador 820 MHz Pentium o su equivalente. **Memoria** 128 megabytes (MB) de RAM **Hard Disk** 10 GB. **Unidad** CD-ROM. **Imagen** VGA o monitor de mayor resolución. **Teclado**. **Tarjeta de Red**	**Procesador** 1.6 GHz Pentium o su equivalente. **Memoria** 256 megabytes (MB) de RAM DDR. **Hard Disk** 40 GB. **Unidad** CD-ROM o DVD. **Imagen** VGA o monitor de mayor resolución. **Teclado**. **Mouse.** **Tarjeta de Red**
Software	
Apache	Apache
Internet Explorer 5.0 o cualquier otro navegador	Internet Explorer 6.0 o cualquier otro navegador
MySQL	MySQL

Tabla 5.3 Requerimientos de implementación de Hardware y Software

5.6.2 ESTRUCTURA DE DIRECTORIOS DEL SISTEMA

La estructura de directorio del sistema se describe a continuación:

Para el Apache se instalará en el directorio:
C:\Program Files\Apache Group

Los archivos de configuración se encontraran en el siguiente directorio:
C:\Program Files\Apache Group\Router_Config

La carpeta que contiene el usuario y contraseña de inicio es:
C:\Program Files\Apache Group\Conf\Router_Config
En esta carpeta se encuentra el archivo de seguridad que maneja el Apache.

La carpeta por default que contiene el servidor TFTP es:
C:\TFTP
Esta carpeta es la que utiliza el Router para enviar o recibir los archivos de configuración.

CONCLUSIONES

En un mundo, donde los cambios se dan de manera acelerada en el área informática, la implementación de políticas de seguridad se convierte en un requisito imprescindible en cada organización; haciendo evidente que deben estar sujetas a las necesidades cambiantes de cada entidad y acoplarse con las nuevas tecnologías.

Hoy en día, la integración de las organizaciones por las diversas tecnologías informáticas son más que una realidad, y las ventajas y limitantes que esto representa obliga a contar con un plan de seguridad y herramientas necesarias para ser implementadas.

Es primordial el hecho de crear un alto grado de conciencia del correcto uso de los recursos de una red informática por parte de los usuarios. Ya que no basta con que los administradores definan una buena gama de políticas de seguridad, si estas no son aplicadas y si los usuarios no acatan y cumplen con las normativas estipuladas.

En base al estudio de mercado realizado, se puede decir que los usuarios cada vez necesitan un nivel mayor de seguridad, es por ello que los administradores o encargados de la protección de las redes deben optar por herramientas que les permitan contar con un nivel adecuado y aceptable de seguridad, aunque todo esto implique una inversión.

Una de las finalidades de hacer uso de un router con características de Firewall es lograr un balance entre seguridad y accesibilidad, ya que de esta manera se obtienen ventajas en cuanto al libre manejo de la información sabiendo que ésta se encuentra completamente segura.

Un router/firewall es parte de la política de seguridad total en una organización, en la cual se definen todos los aspectos competentes al perímetro de defensa. Para que ésta sea exitosa, la organización debe conocer qué protege.

Se demostró que utilizando las características de la IOS Cisco podemos realizar diferentes configuraciones que nos permita minimizar los riesgos de ataques externos. La complejidad de la configuración dependerá de las diferentes técnicas que la empresa u organización estén dispuestas a establecer para proteger su información.

En la actualidad existen una gran variedad de dispositivos que permiten de una u otra forma asegurar el perímetro interno de una red. El prototipo de firewall que presentamos es una opción más que puede ser implementada según sean los requerimientos de las organizaciones.

Una de las aportaciones principales de esta tesis es demostrar que las técnicas que se utilizaron para encriptar o filtrar si son funcionales. Y que fácilmente puede ser adoptadas por las empresas que requieran un prototipo de firewall con IOS Cisco.

Se determinó que el prototipo de firewall usando IOS Cisco puede ser una muy buena solución para pequeñas empresas que requieran una eficaz protección de su red y no dispongan de un gran presupuesto, además si estas empresas cuentan con router estos pueden ser utilizados para la implementación de firewall.

Se concluye que las técnicas de protección estudiadas son soluciones eficientes a los problemas de seguridad, ya que son capaces de detectar, prevenir y disminuir ciertas situaciones de riesgo que inestabilicen el buen funcionamiento de las redes informáticas de las empresas.

Se estima conveniente la defincion de políticas de seguridad asi como, su implementación y correcto seguimiento por parte del adminsitrador de una red. Asi como, crear una en los usuarios un nivel de conciencia tal que permita que ellos hagan un uso adecuado de los recursos de la red.

Como dato relevante a mencionar, se tiene en base a los datos obtenidos por el estudio de mercado que hay mayor preferencia hacia los equipos CISCO ya que se caracterizan por ofrecer seguridad y robustez en sus dispositivos. Muchos administradores en la actualidad ya están optando por nuevas tecnologías que implementan un conjunto de soluciones las cuales simplifican la administración; es de aclarar que aspectos como presupuestos económicos, tamaño de las empresas, políticas de seguridad, etc., son parámetros que deben utilizarse para adoptar alguna tecnología de seguridad existente.

CONCLUSIONES DE TÉCNICAS

- El uso de estas las técnicas anteriormente definidas dependerá de las políticas que las organizaciones desean aplicar para el monitoreo de la información que fluye desde Internet hacia la red interna.

- Es importante mencionar que no es posible aplicar todas las técnicas al mismo dispositivo ya que algunas de ellas no son compatibles entre ellas y además puede generar un cuello de botella.

- El uso de cada técnica dependerá de la estructura de red que se tenga, tamaño de la misma y políticas de seguridad que las organizaciones desean implementar para proteger su información.

- Como punto importante se menciona que existe la posibilidad de implementar todas las técnicas en un mismo dispositivo sin problema alguno, siempre y cuando la IOS Cisco que se esté utilizando soporte cada una de las técnicas.

Es importante tomar en cuenta las capacidades de procesamiento y memoria de los dispositivos, ya que de ello dependería si las diversas técnicas implementadas se convierten en una solución o por el contrario se vuelven contraproducentes para la red misma. Para el caso, los famosos cuellos de botella sería uno de los problemas de implementar todas las técnicas en un dispositivo que originalmente ha sido diseñado para otros fines, tal es el caso de un router.

CONCLUSIONES DE ATAQUES

- El hecho de hablar de ataques informáticos es demasiado complejo ya que día con día se observa una tendencia de crecimiento.

- Actualmente se tiene una diversidad de ataques a redes con el objetivo en común de crear inestabilidad en la funcionalidad de las redes.

  Actualmente se encuentra de moda otro tipo de ataques, mejor conocidos como Ataques de Ingeniería Social en los cuales el atacante busca obtener información de personas que trabajan dentro de la organización. Todo con el fin de clasificar esta información y ver la posibilidad de que sea utilizada en contra de la organización misma. Tal es el caso de: Marcas de equipo, contraseñas, etc., son solo un ejemplo de información que se puede obtener usando la Ingeniería social.

  A lo cual se podría decir que aunque se piense que se está totalmente protegido siempre existe la posibilidad de sufrir un ataque.

GLOSARIO

A

Administrador: Individuo responsable por un sistema o red de sistema.

Antivirus: Programa cuya finalidad es prevenir las infecciones producidas por los virus informáticos así como curar las ya producidas. Para que sean realmente efectivos, dada la gran cantidad de virus que se crean continuamente, estos programas deben actualizarse periódicamente.

ADSL (Asymmetrical Digital Subscriber Line / Línea Digital de Suscriptor Asíncrona): Tecnología de compresión que permite a los hilos telefónicos de cobre convencionales transportar hasta 6 Mbps (megabits por segundo).

AppleTalk: Es la jerarquía de protocolos de Apple Computer para permitir que los equipos Apple Macintosh compartan archivos e impresoras en un entorno de red. Se introdujo en 1984 como una tecnología LAN autoconfigurable. Apple Talk también está disponible en muchos sistemas UNIX que utilizan paquetes comerciales y de libre distribución. El conjunto de protocolos AppleTalk permite compartir archivos a alto nivel utilizando AppleShare, los servicios de impresión y gestores de impresión de LaserWriter, junto con la secuencia de datos de bajo nivel y la entrega de datagramas básicos.

Autenticación: Verificación de la identidad de una persona o de un proceso.

B

Back Orifice: Es una herramienta que consiste de dos componentes una aplicación cliente y una aplicación servidor. La aplicación cliente, corre en una máquina que puede usarse para monitorear y controlar una segunda maquina en la que corre la aplicación servidor.

C

Cracker: Persona que rompe la seguridad en un sistema, intentando acceder sin autorización. Estas personas tienen a menudo malas intenciones, y suelen disponer de muchos medios para introducirse en un sistema.

Caballo de Troya: programa informático que lleva en su interior la lógica necesaria para que el creador del programa pueda acceder al interior del sistema que lo procesa.

CBAC: Control de Acceso Basado en Contexto / Contex Based Access Control. Lleva un registro de las conexiones que se están supervisando, además construye una tabla de estado similar a la que crea los Cisco PIX; además supervisa TCP, UDP y conexiones ICMP. CBAC usa la tabla de estado para crear listas de accesos dinámicas con el fin de permitir devolver el tráfico a través del perímetro de red.

Criptografía: En el contexto de redes informáticas, es la ciencia que estudia los métodos y procedimientos, mediante algoritmos matemáticos, para modificar los datos de tal manera que solamente las personas que tengan la llave adecuada puedan a) tener acceso a la versión original de los mismos (confidencialidad) y b) asegurar que estos datos no han sido modificados entre el remitente y el destino.

Cuotas de disco: Se utilizan para supervisar y limitar el uso de espacio en disco en volúmenes NTFS.

D

Dirección IP: Número entero de 32 bits asignado a un host en una red, definida por el Protocolo Internet en STD 5, RFC 791. Se representa usualmente mediante notación decimal separada por puntos.

DNS (Domain Name System / Sistema de Nombres de Dominios): Base de datos distribuida en línea, usada para la conversión de nombres canónicos a sus respectivas direcciones IP.

DES: Esquema de encriptación simétrico, el cual se creo con el objetivo de proporcionar al público en general, un algoritmo de cifrado normalizado para redes.
3DES: Basado en 3 iteraciones sucesivas del algoritmo DES consiguiendo con ello una clave de 128 bits. Además es compatible con DES simple.

E

Encriptado: Es el tratamiento de los datos contenidos en un paquete a fin de impedir que nadie excepto el destinatario de los mismos puede leerlos. Hay muchos tipos de cifrado de datos, que constituyen la base de la seguridad de la red.

F

FTP (File Transfer Protocol / Protocolo de Transferencia de Archivos): Servicio de TCP/IP que permite transferir archivos desde una maquina hacia otra a través de Internet.
Firewall (muralla de fuego): Equipo dedicado que es utilizado para comunicar la red privada con la red pública. Este equipo es un ordenador especializado que controla y administra el flujo de información entre la red privada interna y el mundo exterior. (Cortafuegos). Es un dispositivo hardware y software, que conecta entre dos o más redes y permite limitar el acceso a los sistemas en los dos sentidos.
Frame-relay: Tecnología de transporte de datos por paquetes utilizada muy comúnmente en las conexiones por líneas dedicadas.
Failover: Es un modo de operación de backup en el cual las funciones de un componente del sistema son asumidas por un segundo componente del sistema cuando el primero no se encuentra disponible debido a un fallo ó un tiempo de parada preestablecido. Es usado para hacer a los sistemas más tolerantes a fallos, y de esta forma hacer el sistema permanentemente disponible.

G

Gusanos: Programa que hace copias de si mismo sobre distintas maquinas interconectadas por la red.

H

Hacker: Una persona alcanza un conocimiento profundo sobre el funcionamiento interno de un sistema, de una PC o de una red. Este término se suele utilizar indebidamente como peyorativo, cuando sería más correcto utilizar el término "cracker".

I

Ingeniería Social: Arte de convencer a la gente de entregar información que no corresponde.

Internet: Grupo de computadoras interconectadas por un medio de redes que pueden comunicarse a través de un conjunto de protocolos llamados TCP/IP.

Internetworking: Involucra conectividad entre dos o más computadoras en la red con algunos dispositivos de ruteo para intercambiar tráfico, además de guiar el tráfico por un camino adecuado. Generalmente utiliza dispositivos llamados Routers (originalmente Gateways).

IPX: Conectan una red de computadoras utiliza Protocolos de capa 3.

IPv6 (IP versión 6): Propuesta para aumentar los números IP disponibles, utilizando seis grupos de números en lugar de cuatro.

IP (Protocolo): Protocolo de conmutación de paquetes que realiza direccionamiento y encaminamiento. Protocolo no orientado a la conexión y envía paquetes sin esperar la señal de confirmación por parte del receptor. IP es el responsable del empaquetado y división de los paquetes requerido por los niveles físicos y de enlace de datos del modelo OSI. Cada paquete IP está compuesto por una dirección de

origen y una de destino, un identificador de protocolo, un checksum (un valor calculado) y un TTL (tiempo de vida, del inglés *time to live).*

L

LAN (Local Area Network / Red de Area Local): Grupo de computadoras y periféricos conectados entre si y que se encuentran localizados en un área física próxima, por lo que pueden mejorar los protocolos de señal de la red para llegar a velocidades de transmisión de hasta 100 Mbps (100 millones de bits por segundo).

N

NAP (Network Access Point / Centro de Acceso a la Red): Punto de interconexión para intercambio de datos de dos o más conexiones pertenecientes a distintas organizaciones o ISPs.

NetBus: Es un programa troyano de administración remota similar al BackOrifice, mientras el usuario este conectado a Internet y en su computadora se este corriendo esta aplicación nadie desde cualquier lugar puede tener acceso al programa cliente del NetBus sin la autorización y consentimiento previo del usuario.

Network: Una red de ordenadores es un sistema de comunicación de datos que conecta entre sí sistemas informáticos situados en diferentes lugares. Puede estar compuesta por diferentes combinaciones de diversos tipos de redes.

NBAR (Network Based Application Recognition / Aplicación de Red Basado en Reconocimiento): Usado normalmente para llevar a cabo funciones de QoS en un enrutador.

P

Protocolo: Es una Descripción formal del formato de los mensajes y las reglas que deben ser seguidas para intercambiar dichos mensajes.

Puerto: Camino especifico para información de control o datos entre dos computadoras.

PAP (Password Authentication Protocol / Protocolo de Autentificación por Password): Permite al sistema verificar la identidad del otro punto de la conexión mediante password.

PIX (Private Internet Exchange/ Intercambio de Internet Privado): Es una solución de seguridad de hardware/software especializada que entrega la seguridad de alto nivel sin impactar la actuación de la red. Es un sistema híbrido porque usa los rasgos de ambos el paquete que se filtra y tecnologías de servidor de apoderado.

Politica de Seguridad Informatica (PSI): Es una herramienta organizacional creada con el fin de concienciar a cada uno de los miembros de una organización sobre la importancia y la sensibilidad de la información y servicios críticos que favorecen el desarrollo de la organización y su buen funcionamiento.

POP (Post Office Protocol / Protocolo de Oficina de Correos): Programa cliente que se comunica con el servidor, identifica la presencia de nuevos mensajes, solicita la entre de los mismos y utiliza al servidor como oficina despachadora de correo electrónico cuando el usuario envía una carta.

PPP (Point to Point Protocol / Protocolo Punto a Punto): Implementación de TCP/IP por líneas seriales (como en el caso del módem). Es más reciente y complejo que SLIP.

Proxy: Una substitución de direcciones, usado para limitar la información de direcciones disponibles externamente.

R

RDSI (Red Digital de Servicios Integrados): Tecnología en plena evolución que está empezando a ser ofrecida por las compañías telefónicas más Importantes. Combina servicios de voz y digitales a través de la red en un solo medio, haciendo posible ofrecer a los clientes servicios digitales de datos así como conexiones de voz a través de un solo "cable". Los estándares de RDSI los especifica la CCITT.

Router (Direccionador): Dispositivo que distribuye tráfico entre redes. La decisión sobre a dónde enviar se realiza basándose en información de nivel de red y tablas de direccionamiento.

RADIUS: El Servicio de usuario de acceso telefónico de autenticación remota es un protocolo cliente-servidor de autenticación de seguridad, ampliamente utilizado por los proveedores de servicios Internet en otros servidores de acceso remoto. RADIUS es el medio más frecuente de autenticación y autorización de usuarios de acceso telefónico y de redes de túnel.

S

Sniffer: Herramienta utilizada para el rastreo de tráfico en una red de datos.

Scanner: Herramienta de software para la evaluación de sistemas, esta herramienta averigua que conexiones son posibles con ese sistema, comúnmente evalúa los puertos en busca de “agujeros”.

Switched Multimegabit Data Service (SMDS): Tecnología de Gestión de redes de alta velocidad ofrecida por las compañías telefónicas.

SMTP (Simple Mail Transfer Protocol / Protocolo Simple de Transferencia de Correo): Protocolo estándar de Internet para intercambiar mensajes de correo electrónico.

Spam:

SSL (Secure Socket Layer / Capa de Seguridad): Estándar para transacciones electrónicas encriptadas que está siendo ampliamente utilizado para hacer negocios vía la Red

T

TCP (Transmission Control Protocol / Protocolo de control de Transmisión): Uno de los protocolos más usados en Internet. Es un protocolo de capa de transporte.

TCP / IP (Transmission Control Protocol / Internet Protocol): Arquitectura de red desarrollada por la "Defense Advanced Research Projects Agency" en USA, es el conjunto de protocolos básicos de Internet o de una Intranet.

TELNET: Protocolo perteneciente a TCP/IP que provee soporte para sesiones terminal remota sobre una red Tecnología:

TACACS (Terminal Access Controller Access Control System): Sistema de control de acceso al TAC. Protocolo de autenticación, desarrollado por la comunidad DDN, que provee autenticación de acceso remoto y servicios relacionados, como registro de eventos. Las contraseñas de usuario se administran en una base de datos central, en vez de en routers individuales, lo que ofrece una solución de seguridad de red fácilmente escalable.

U

URL (Uniform Resource Locator / Localizador Uniforme de recursos): Sistema de direccionamiento estándar para archivos y funciones de Internet, especialmente en el Word Wide Web.

V

Virus: Fragmento de código que al ejecutarse inserta copias de sí mismo en otros ejecutables. Estos programas pueden causar problemas de diversa gravedad en los sistemas que los almacenan.

VPN: Es una red privada que se extiende, mediante un proceso de encapsulación y en su caso de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte.

W

WAN (Wide Area Network / Red de Area Amplia): Red en que los componentes se encuentran físicamente distantes unos de otros.
Web: Servicio de gran escala que permite al usuario "Navegar" a través de la información. El Web ofrece un sistema de hipermedios que sirven para acceder texto, gráficos, audio, video, etc.

X

X.25: Se usa en una gran cantidad de redes públicas en todo el mundo para conectar LAN´s privadas a redes públicas de datos. Desde el punto de vista de X.25, la red funciona como lo hace el sistema telefónico. En X.25, cada host se conecta a un switch que tendrá la obligación de enrutar los paquetes de los diferentes enlaces. Para comprender mejor esto, veamos una comparación de X.25 contra el modelo de referencia OSI.

FUENTES DE INFORMACIÓN

BIBLIOGRAFÍA

a) Libros

[1] Roberto Hernández Sampieri, Carlos Fernández Collado, Pilar Baptista Lucio, **Métodología de la Investigación**, McGraw Hill/Interamericana Editores, S.A. de C.V., Tercera Edición, 2003.

[2] Brent Chapman and Elizabeth D. Zwicky, **Construya Firewalls Para Internet**, McGraw Hill, Inc, Primera Edición, 1997.

[3] Richard A. Deal, **Cisco Router Firewall Security**, Cisco Press, Primera Edición, Agosto 2004.

[4] Brian Hill, **Cisco Manual de Referencia, Mc Graw Hill,** Primera Edición,

b) Tesis

[5] Luis Alberto Orellana, Rafael Hernández, **Seguridad de Redes**, Octubre del 2003.

[6] Erick Alfredo Flores, Ricardo Ernesto Castillo, **Seguridad y Protección de LAN Utilizando un Firewalls Basado en servidor Proxy,** Octubre de 1999.

[7] Luis Alberto Orellana Benavides, Rafael Cristobal Hernández, **Seguridad en Redes de datos,** Octubre de 2003.

c) Sitios de Internet

[8] http://www.countersiege.com/doc/pfsync-carp (Visitado el Sábado 4 de Diciembre de 2004). Countersiege Systems Corporation.

[9] http://perso.wanadoo.es/aniorte_nic/apunt_metod_investigac4_9.htm (Visitado el Domingo 5 de Diciembre de 2004). Página personal sobre la Licenciatura en Enfermería de: NICANOR ANIORTE HERNÁNDEZ.

Debido a previsibles problemas con el servidor, en cuanto al espacio disponible para alojar la Web, te recomiendo que guardes la nueva dirección, si prevés accesos posteriores:

http://perso.wanadoo.es/nicanorap/

[10]http://www.cisco.com/en/US/products/hw/routers/ps221/prod_bulletin09186a0080161145.html (Visitado el Domingo 5 de Diciembre de 2004). Cisco System.

[11]http://info.cisco.de/global/DE/solutions/smb/produkte/1760_modular_access_router.pdf (Visitado el Domingo 5 de Diciembre de 2004). Cisco System.

[12] http://www.dei.uc.edu.py/tai2002-2/firewall/firewalls.html (Visitado el martes 7 de diciembre de 2004). Departamento de Electrónica e Informática. Universidad Católica Nuestra Señora de La Asunción.

[13]http://www.mailxmail.com/curso/informatica/delitosinformaticos/capitulo33.htm (Visitado Viernes 6 de mayo de 2005).

[14]http://www.derechotecnologico.com/estrado/estrado004.html (Visitado Viernes 6 de mayo de 2005). Página personal de Jeimy J. CANO.

[15] http://www.belt.es/expertos/experto.asp?id=2391 (Vistado Lunes 9 de mayo de 2005). Página de Belt Ibérica S.A. Analistas de Prevención.

[16]www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_category_home.html (Visitado Sabado 3 de septiembre 2005).

[17]http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html (Visitado Lunes 5 de septiembre 2005).

[18]http://mural.uv.es/emial/informatica/html/IDS.html (Visitado Lunes 9 de mayo de 2005). Página de Universidad de Valencia.

[19]http://www.maestrosdelweb.com/editorial/phpintro/ (Visitado Sabado 23 de Julio de 2005).

[20]http://www.augcyl.org/glol/old/N_1/apache.html (Visitado Sabado 23 de Julio de 2005).

[21]http://www.software-shop.com/Productos/MySQL/mysql.html (Visitado Sabado 23 de Julio de 2005).

[22]http://www.faqs.org/rfcs/rfc3768.html , http://www.cisco.com/en/US/products(ps6550/products (Visitado el 3 de noviembre de 2005).

ANEXOS

ANEXO 1. LISTADO DE PREGUNTAS DE LA ENCUESTA

1. ¿A qué sector pertenece la empresa en la que usted trabaja?

Sector	Total	Porcentaje
ONG		
Salud		
Gobierno		
Financiero		
Transporte		
Educación		
Tecnología		
Servicios Varios		
Telecomunicaciones		
Otros		
Total		

2. ¿Si usted eligió la opción Otros en la pregunta anterior, favor Especifique?

3. ¿Qué prioridad en el tema de Seguridad, asigna(ría) usted como Administrador en su red para asegurar la protección de los Datos?

Prioridad	**Total**	**Porcentaje**
Extrema		
Alta		
Moderada		
Mínima		
Ninguna		
No sabe		

4. Por el creciente acceso a Internet, ha incrementado la posibilidad de que personas Ajenas a la organización puedan acceder a la información de su empresa. ¿Qué considera la organización como peligros más apremiante?

Peligros Apremiantes	**Total**	**Porcentaje**
Acceso No autorizado por personal Interno		
Robo de Información confidencial		
Spamming de correo electrónico		
Abuso del acceso de Internet		
Modificación de Páginas Web		
Penetración de Sistemas		
Denegación de Servicio		
Spyware		
Adware		
Virus		
Otros		
Total		

5. ¿Si usted eligió la opción Otros en la pregunta anterior, favor Especifique?

6. Tecnologías de seguridad que utilizan actualmente para asegurar la información de su empresa

Tecnologías	**Total**	**Porcentaje**
Firewall basado en Software utilizando Windows		
Firewall basado en Software utilizando Linux		
Router utilizado como Firewall		
Redes privadas virtuales (VPN)		
Certificados Digitales		
Software antivirus		
Servidor Proxy		
Firewall		
Otros		
Total		

7. ¿Si usted eligió la opción Otros en la pregunta anterior, favor Especifique?

8. ¿Qué equipo de internetworking posee en su organización?

Tipo de Internetworking	Total	Porcentaje
IDS		
IPS		
Router		
Firewall		
Switch		
Hub		
Total		

9. ¿Si usted utiliza Router, éste que marca es?

Marca	Total	Porcentaje
Motorola		
Netgear		
LinkSys		
D-Link		
3COM		
Cisco		
Otro		
Total		

10. ¿El router es arrendado por algún Proveedor de Equipo?

Respuesta	Total	Porcentaje
Si		
No		
Total		

11. ¿Quién realiza la configuración de su Router?

Respuesta	Total	Porcentaje
Alguna Empresa especializada en Seguridad		
Proveedor de Servicio de Internet		
Personal de su Organización		
No se poseen Router		
Total		

12. ¿Cuál ha sido la inversión monetaria hasta la fecha en materia de seguridad?

Inversión	**Total**	**Porcentaje**
0 - $1,000		
$1,001 - $3,000		
$3,001 - $5,000		
$5,001 o más		
Total		

13. Hoy en día podemos usar diferentes tecnologías que nos permita asegurar la información de las empresas. ¿Qué tecnologías de seguridad podría utilizar e su organización?

Tecnologías	**Total**	**Porcentaje**
Servidor Proxy		
Software antivirus		
Firewall		
Router utilizado como Firewall		
Firewall basado en Software utilizando Windows		
Firewall basado en Software utilizando Linux		
Sistema de detección de intrusos		
Anti Spam		
Certificados Digitales		
Redes privadas virtuales		
Otros		
Total		

14. ¿Si usted eligió la opción Otros en la pregunta anterior, favor Especifique?

15. ¿Qué equipo de internetworking utilizaría para proteger su organización de posibles ataques externos?

Equipo	**Total**	**Porcentaje**
IDS		
IPS		
Router		
Firewall		
Switch		
Total		

16. ¿De cuánto son los fondos anuales con los que cuenta, para implementar algunas de las técnicas de seguridad antes mencionadas?

Inversión	**Total**	**Porcentaje**
0 - $1,000		
$1,001 - $3,000		
$3,001 - $5,000		
$5,001 - o más		
Total		

ANEXO 2. ESPECIFICACIONES TÉCNICAS DEL ROUTER [4]

COMPONENTES INTERNOS Y EXTERNOS

Los componentes internos de los dispositivos de Cisco varían ligeramente según la función del dispositivo, los requisitos de potencia, el factor de forma y la modularidad, pero hay unos cuantos componentes básicos que se incluyen casi siempre. En muchos casos, los enrutadores o conmutadores se asemejan a PC especializados, con componentes parecidos utilizados para fines semejantes.

Sin embargo, prácticamente todos los elementos de un dispositivo de Cisco están diseñados especialmente no sólo para los productos de Cisco, sino, en la mayor parte de los casos, para un determinado modelo de producto de esta empresa. Por tal motivo, cuando se adquieran componentes de hardware, como ampliaciones de memoria, deben elegirse para un equipo Cisco en particular, lo que a menudo supone pagar más.

Además de los internos, los componentes externos de los equipos de Cisco también son bastante variables, dependiendo de nuevo del modelo de dispositivo de que se trate.

COMPONENTES INTERNOS

Los componentes internos más comunes son los módulos RAM, la memoria flash, la memoria ROM, la UCP, el panel posterior y la RAM no volátil (NVRAM, NonVolatile RAM).

- MODULOS RAM

Los dispositivos de Cisco utilizan RAM dinámica (DRAM, Dynamic RAM), igual que los PC, como memoria de trabajo. La memoria RAM de estos equipos guarda la configuración en curso, denominada configuración de ejecución o running config y la versión actual del sistema operativo (IOS, Intemetwork Operating System), que es el que funciona en la mayoría de los equipos de Cisco.

Por suerte, en la mayoría de los casos en los dispositivos de Cisco no se necesita tanta memoria como la requerida habitualmente en los sistemas operativos de las PC

de hoy. Como cantidad típica de memoria RAM necesaria para la mayoría de los enrutadores se manejan cifras de 16 MB.

Los dispositivos de Cisco utilizan comúnmente módulos de memoria en línea simples (SIMM, Single Inline Memory Modules) y dobles (DIMM, Dual Inline Memory Modules) para la RAM, de igual forma que un PC; pero en general no son los DIMM o SIMM estándar que se podrían comprar para un PC. Se trata en este caso de componentes especialmente fabricados para el dispositivo de Cisco (en general, se acoplan en el módulo en un lugar diferente), por lo que cuestan bastante más que los normales.

- MEMORIA FLASH

La memoria flash se utiliza en los dispositivos de Cisco de forma similar al disco duro en un PC. Esta memoria contiene la IOS guardada y se usa para almacenamiento más permanente que la RAM, ya que la información no se pierde cuando se desconecta el enrutador. La memoria flash existe en dos variantes principales dentro de los equipos de Cisco: SIMM o DIMM, que pueden insertarse como una RAM estándar, o tarjetas PCMCIA de memoria flash (o PC Cards, si se prefiere).

Una vez más, con independencia de cómo se inserte, la memoria flash forma parte obligatoria del equipo de Cisco. Además, sólo el hecho de que contenga una ranura PCMCIA, que es un estándar de la industria, no significa que pueda utilizarse cualquier tipo antiguo de tarjeta de memoria flash. Como sucedía con los módulos RAM, normalmente se requiere una tarjeta adaptada al modelo concreto de dispositivo de que se trate.

- ROM

La memoria ROM de un dispositivo de Cisco se emplea normalmente para guardar una versión de copia de seguridad de la IOS para usarla cuando no pueda arrancarse el dispositivo por otras vías. La memoria ROM contiene el código de monitor ROM (Rommon, ROM Monitor), que se utiliza si el IOS de la memoria flash se ha corrompido y no puede ejecutarse, o bien para tareas de diagnóstico y reconfiguración de bajo nivel (por ejemplo, si alguien cambia la contraseña y bloquea el enrutador). Como la ROM es, por definición, una memoria de sólo lectura, para ampliar el equipo a una nueva versión de ROM normalmente se debe extraer el circuito ROM viejo del zócalo donde se encuentra e insertar en su lugar el nuevo chip de ROM.

- UCP

La UCP (unidad central de procesamiento) se utiliza con el mismo objetivo que en un PC: es el «cerebro» del dispositivo. La mayoría de los equipos de Cisco llevan a cabo númerosas operaciones de cálculo por software, de las que se encarga la UCP. Cisco utiliza muchos modelos diferentes de UCP en sus distintos equipos, dependiendo del uso pretendido de los mismos. En un enrutador, la UCP es especialmente importante, porque la mayoría de las funciones de un enrutador son desempeñadas por software y la UCP tiene una influencia espectacular en el rendimiento. En los Routers, la UCP suele ser menos importante, porque la mayoría de los cálculos de un Router se llevan a cabo en elementos especializados de hardware conocidos como circuitos integrados específicos de la aplicación (ASIC, Application-Specific Integrated Circuits).

- PANEL POSTERIOR

El término «ancho del panel posterior» aparece muy a menudo en las conversaciones sobre los dispositivos de redes (normalmente router). El panel posterior es como el bus por el que todas las comunicaciones de redes viajan al interior del dispositivo de red. Este panel tiene una importancia fundamental en los conmutadores y otros dispositivos de alta densidad de puertos. Para conocer su capacidad bastan unos sencillos cálculos matemáticos.

En un enrutador estándar de baja densidad de puertos, la velocidad del panel posterior tiene una relevancia mínima. La velocidad en paquetes por segundo (PPS) en un enrutador tiene mucho menos que ver con la del panel posterior que con la velocidad del procesador. Normalmente, un enrutador nunca funciona a la velocidad del cable. En conmutadores y otros dispositivos de alta densidad de puertos, sin embargo, el panel posterior es una de las consideraciones de diseño más importantes.

- NVRAM

La memoria RAM no volátil (NVRAM, Non- Volatile RAM) es una clase de RAM que no pierde información cuando se produce una caída de tensión. La cantidad de NVRAM en la mayoría de los dispositivos de Cisco es muy pequeña (normalmente, entre 32 y 256 KB), Y se utiliza para guardar la configuración utilizada en el arranque, denominada configuración de inicio.

COMPONENTES EXTERNOS

Algunos de los dispositivos externos más comunes son el puerto de consola, el puerto auxiliar (AUX), los puertos Ethernet, los puertos serie y las ranuras PCMCIA.

- PUERTO DE CONSOLA

El puerto de consola es la interfaz principal de la mayoría de los dispositivos de Cisco (excepto las estaciones base Cisco Aironet). Este puerto se utiliza para acceder a lOS y obtener la configuración inicial, y contiene un único conector RJ-45. El puerto de consola es en realidad un puerto serie asíncrono de baja velocidad (como los puertos serie de los PC) que tiene una configuración de pines y un tipo de cable especiales, el puerto de consola también repite todas las notificaciones que se producen, lo que hace de él una herramienta muy valiosa para la localización de averías.

- PUERTO AUXILIAR

Resaltado con la etiqueta «AUX», el puerto auxiliar es un puerto serie asíncrono de baja velocidad que se usa normalmente para conectar un módem a un dispositivo de Cisco que permita la administración remota. La mayoría de los equipos de Cisco incluyen un puerto AUX.

- PUERTO ETHERNET

Los puertos Ethernet 10BaseT pueden estar o no presentes en un dispositivo de Cisco (según el modelo de que se trate), aunque en la mayoría de estos equipos existe al menos uno de tales puertos. Los puertos 10BaseT suelen suministrarse con el conector de estilo RJ-45 estándar, aunque también se puede tener un puerto de interfaz de unidad de conexión (AUI, Attachment Unit Interface). El puerto AUI es un conector DB-15 (el mismo que el conector del mando de juegos de un PC) que requiere el uso de un transceptor (abreviatura de transmisor/receptor) para establecer una conexión con la red. Ello permite el uso de otros tipos de cableado Ethemet (como cable coaxial).

- PUERTO SERIE

Varios modelos de dispositivos de Cisco incluyen interfaces serie de baja y alta velocidad. Los enrutadores usan clásicamente una interfaz serie síncrona de alta velocidad para la comunicación con una unidad de servicios de canal/unidad de servicios de datos (CSU/DSU, Channel Services Unit/Data Services Unit) de la red WAN, mientras que los servidores de acceso suelen tener múltiples puertos serie asíncronos de baja velocidad para comunicación con módems.

- RANURAS PCMCIA

Algunos dispositivos de Cisco (como el enrutador 3660) incluyen ranuras PC-CIA (comúnmente llamadas PC Cards), de manera que será posible añadir fácilmente memoria flash. Si los enrutadores del usuario tienen esta dotación, extender el lOS a múltiples enrutadores del mismo modelo resultará extraordinariamente sencillo. En lugar de tener que usar TFTP para transferir la imagen lOS a cada enrutador bastará con cargarlo en una PC Card y transferirlo a los enrutadores desde la tarjeta.

- MODULARIDAD

Los dispositivos de Cisco pueden darse en dos configuraciones básicas: fija o modular. Los dispositivos fijos no pueden ampliarse. Simplemente se suministran con un número y un tipo de interfaces preestablecidos (como el enrutador 2501) y no es posible extenderlos con nuevas interfaces. En cambio, los dispositivos modulares se entregan con ranuras de módulos que hacen posibles ampliaciones.

Los dispositivos modulares pueden agregarse a cuatro modelos básicos. En su forma más sencilla, el dispositivo simplemente acepta tarjetas de línea (semejantes a las tarjetas de ampliación de los PC), denominadas tarjetas de interfaz WAN (WIC, WAN Interface Cards), para añadir nuevas funciones. Este dispositivo se proporciona normalmente con un número preestablecido de ranuras de tarjetas para ampliación.

El segundo tipo de dispositivo utiliza una ranura de tarjetas mayormente denominada módulo de red, que incluye normalmente una o más interfaces LAN o WAN y puede tener ranuras en el módulo de red para otras tarjetas WIC.

La tercera clase utiliza un componente aún mayor (denominado blade, o «cuchilla», en argot), al que Cisco puede atribuir diferentes nombres dependiendo del modelo del dispositivo en cuestión. Estos componentes admiten generalmente un tipo de interfaz de red cada uno, pero pueden recibir un número elevado de puertos por módulo.

Finalmente, el último tipo de dispositivo tiene una combinación de tarjetas WIC y de ranuras de módulos de red. Esta configuración permite una gran libertad para elegir las prestaciones. Un buen ejemplo sería el enrutador 2611, que en modo estándar se suministra con dos puertos Ethemet, dos ranuras WIC y una sola ranura de módulo de red. Con esta gran modularidad es posible tener un enrutamiento 2611 entre dos redes Ethemet independientes y comprar dos tarjetas WIC serie síncronas de puerto dual, lo que permite la posibilidad de enrutar a través de cuatro enlaces totales Frame Relay y luego añadir un módulo de red ATM DS3 en la ranura libre de módulos de red.

- PUERTO AUX

El puerto AUX es similar al puerto de consola en lo que se refiere a las conexiones físicas. La diferencia verdadera entre los dos es la manera de usarlo. El puerto AUX puede utilizarse como una conexión de terminal, aunque propiamente no lo sea. Si se quiere utilizar para este fin, se tiene que conectar un cable RJ-45 al puerto AUX y utilizar un adaptador DTE DB-25 o DB-9 (normalmente incluido junto con el enrutador).

La forma más común de usar un puerto AUX consiste en conectarlo a un módem. Para ello se seguirá necesitando el cable inversor, pero esta vez se usa un adaptador DCE. Puede advertirse que existen dos clases de adaptadores DCE: de

módem y de no módem. El que se quiere aquí es el de módem; el otro ha quedado obsoleto.

- PUERTO AUI

Normalmente, todo lo que se necesita para conectar un cable UTP a un puerto AUI es un transceptor de cierta calidad. Basta con enchufar el transceptor al puerto AUI y el cable UTP a la toma RJ-45 del transceptor. Alternativamente puede usarse un cable AUI para conectarse con un transceptor independiente, pero usando en esencia el mismo procedimiento. Si es preciso realizar una conexión a una red Ethernet coaxial, el procedimiento se complica un poco. Sin embargo, sigue bastando con conectar el transceptor al medio como cualquier otro dispositivo y luego enchufar el transceptor al puerto AUI en el enrutador.

- SERIE 1700 [4]

La serie 1700 es la línea más básica de enrutadores para sucursales comercializada por Cisco. Está pensada para sucursales y oficinas que necesitan un amplio soporte para tecnologías de enrutamiento, una gama amplia de opciónes de interfaz, capacidad de manejo de múltiples protocolos, integración de voz y uso de redes privadas virtuales y cortafuegos, pero sin llegar a los niveles de rendimiento y prestaciones de otras líneas de gama superior.

La serie 1700 ofrece esencialmente los mismos conjuntos de características disponibles en la serie 1600, como soporte DHCP, NAT, QoS, listas de acceso, prestaciones de redes privadas virtuales/cortafuegos y capacidades de enrutamiento multiprotocolo (IP, IPX, AppleTalk y SNA). Además, se ofrece con un procesador de rendimiento superior que en la serie 1600, incluye un amplio soporte para protocolos de enrutamiento (como RIP, IGRP, EIGRP, OSPF y BGP) y en los modelos 1750, también soporte para voz.

Esta serie se compone de cuatro modelos: 1720, 1750, 1750-2V y 1750-4Y. Al ser modular, todos ellos admiten las mismas tarjetas de interfaz, que comparten además con los enrutadores de las series 1600, 2600 y 3600, lo que permite proteger la inversión si se necesitan ampliaciones futuras de la infraestructura, además de

simplificar la disposición física. Entre las tarjetas de interfaz disponibles en la serie 1700 se incluyen las siguientes:

- Interfaz serie monopuerto (síncrona y asíncrona; 2,048 Mbps).
- Interfaz serie de 2 puertos (síncrona y asíncrona; 2,048 Mbps).
- Interfaz serie de 2 puertos de baja velocidad (128 Kbps) (síncrona y asíncrona). Interfaz TI monopuerto con CSU/DSU integrada.
- Interfaz 56 Kbps monopuerto con CSU/DSU integrada.
- Tarjeta de interfaz RDSI de acceso básico monopuerto.
- Tarjeta de interfaz RDSI de acceso básico monopuerto con NT-1 integrado. Interfaz ADSL monopuerto.
- Interfaz Ethernet monopuerto (lO Mbps).

Además, los enrutadores 1750 admiten una tarjeta de interfaz de voz de dos puertos. Los cuatro modelos de la línea de enrutadores 1700 varían ligeramente en su soporte para tarjetas de interfaz y en sus conjuntos de características. Seguidamente se detallan las diferencias en estos modelos:

1720. Incluye una sola interfaz Ethernet 10/100, dos ranuras WIC y una única ranura de ampliación para módulos VPN. Los conjuntos de características de lOS disponibles incluyen soporte para DHCP, NAT/PAT, SNMP, listas de acceso, gestión de colas avanzada, QoS, TACACS+, RADIUS, compresión, VPN, IPSec, servicios de cortafuegos, IPX, SNA y AppleTalk.

1750. Incluye una sola interfaz Ethernet 10/100, tres ranuras WIC y una única ranura de ampliación para módulos VPN. Los conjuntos de características de lOS disponibles incluyen soporte para todas las prestaciones del 1720, además de integración voz/fax (con la inclusión de un equipo de ampliación para voz).

1750-2V. Incluye una única interfaz Ethernet 10/100, tres ranuras WIC y una única ranura de ampliación para módulos VPN. Los conjuntos de características de lOS disponibles incluyen soporte para todas las prestaciones del 1720, además de integración voz/fax, y utilizan un DSP que admite hasta dos tarjetas de interfaz voz/fax.

1750-4V. Incluye una única interfaz Ethernet 10/100, tres ranuras WIC y una única ranura de ampliación para módulos VPN. Los conjuntos de características de lOS disponibles incluyen soporte para todas las prestaciones del 1720, además de integración voz/fax, utilizando un DSP que admite hasta cuatro tarjetas de interfaz voz/fax.

Con la modularidad disponible en la serie 1700, unida a la capacidad de integración de voz y datos, la serie 1700 está pensada sobre todo para oficinas y sucursales pequeñas que necesiten una solución versátil para enrutamiento y voz.

ANEXO 3. ESPECIFICACIONES TÉCNICAS DE IOS Cisco [4]

CISCO IOS FIREWALL

El conjunto de características Cisco lOS Firewall permite que la mayoría de los enrutadores estándar de Cisco, desde la serie 800 a la 7500, usen prestaciones avanzadas de seguridad para el soporte de redes, con o sin un dispositivo de hardware dedicado (como un PIX Firewall).
Este conjunto de características añade una serie de herramientas de seguridad complementarias a la línea de enrutamiento de Cisco, entre las que se incluyen las siguientes:

- Control de acceso basado según el contexto (CBAC, Context-Based Access Control), una propiedad que permite ejercer un control del tráfico basado en cada aplicación. Permite dinámicamente que se establezcan sesiones desde una dirección interna y deniega las sesiones originadas en anfitriones externos.

- Características de detección de intrusiones que informan sobre las violaciones de seguridad y los ataques comunes. Soporte de autenticación de conexiones telefónicas TACACS+ y RADIUS.

- Características de detección y prevención de situaciónes de denegación de servicio y de eliminación de los paquetes relacionados con un ataque de de negación de servicio.

- Bloqueo de applets Java.

- Soporte para redes privadas virtuales, encriptación, IPSec y QoS.

- Alerta en tiempo real.

- Capacidad de vigilancia para detallar violaciones del sistema, incluidas in formaciones de dirección y marcas de tiempo.

- Listas de acceso básicas y avanzadas.

- Control sobre acceso de usuarios mediante dirección IP e interfaz.

- Listas de acceso basadas en tiempo.

Estas características convierten a un enrutador Cisco corriente en un formidable cortafuegos de hardware para las redes que no pueden permitirse contar con un dispositivo de cortafuegos dedicado o que sólo necesitan la seguridad adicional que proporciona esta propiedad.

IOS **[4]** páginas 337 a 374 **[10], [11]**

IOS son las siglas de Internetworking Operating System (sistema operativo de interred), el sistema operativo de los dispositivos de Cisco. El sistema IOS controla todas las funciones del dispositivo, desde las listas de acceso a las colas y suministra una interfaz de usuario para la gestión del dispositivo.

VERSIONES Y ESTRUCTURAS DE VERSIONES DE IOS

El sistema IOS de Cisco ha pasado por varias revisiones importantes desde su primera aparición, y de uno u otro modo parece destinado a experimentar constantes modificaciones.
Cada imagen de IOS tiene un conjunto de características especial. En general, añadir nuevas características a un enrutador significa sencillamente descargar una nueva imagen IOS (aunque, en algunos casos, puede requerirse un hardware adicional).
Estas diferencias en las imágenes de IOS se reflejan en la convención de nombres para IOS que utiliza Cisco.

Los números de versión IOS principal pueden parecer un tanto complejos, pero no son difíciles de entender una vez que se conoce el método que hay detrás de esta parafernalia de nombres de Cisco. Aunque este método no es válido para todas las versiones de IOS, funciona en la mayoría de ellas.

LOS NOMBRES DE LAS VERSIONES

El proceso indicado tomando como ejemplo la versión 12.0(3a)T. Primero, se da al IOS un número correspondiente a la versión principal, en este caso, 12.0. Después se indica entre paréntesis la revisión de mantenimiento, (3a), donde la a indica que esta revisión ha sido reconstruida (normalmente, por la presencia de un error importante). Por último, el campo ED indica el tipo de tecnología para el que ha sido diseñado el IOS. En este caso, la T indica tecnología consolidada o dispositivos multifuncionales (normalmente modulares).

Las versiones ED no son las principales para IOS, sino que se utilizan para añadir características y nuevas funciones al IOS y suelen tener errores. En muchos casos, sin embargo, terminan por usarse en los entornos corrientes, ya que proporcionan las características avanzadas no disponibles en la versión principal.

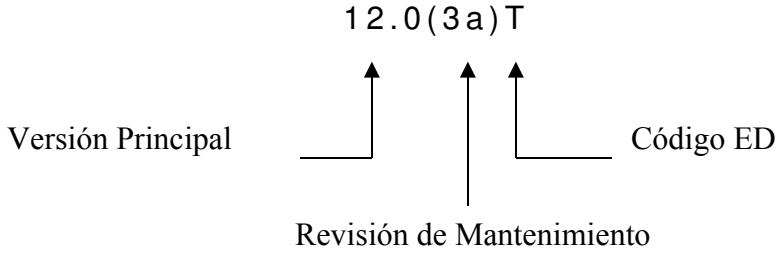


Figura A-3.1 A continuación se muestra el significado del número de versión de IOS Cisco.

En la siguiente Tabla se describen todos los campos ED estándar.

Código ED	Descripción
A	Servidor de acceso
D	Xdsl
E	Conjunto de características de empresa
H	SDH/SONET
N	Multiservicio (voz, vídeo, etc.)
S	Proveedor de servicios
T	Tecnología consolidada
W	Conmutación ATM/WAN/L3

Tabla A-3.1 Descripción de campos ED estándar

En lo referente a la convención de nombres de archivos, Cisco toma la versión de lOS y luego prepara un conjunto más complejo añadiendo otras informaciones específicas.

Para aclararlo, el nombre de archivo podría aparecer en una imagen lOS como algo similar a c4500-js40_l20-3t.mz, lo cual a decir verdad, no resulta muy cómodo. Tampoco aquí es todo tan confuso, una vez que se conoce el origen de la convención de nombres.

A continuación el desglose:

El término c4500 corresponde a la plataforma y, en este caso, indica que la imagen corresponde a un enrutador de las serie 4500.
El valor js40 indica un conjunto de características (que se mostrara en la Tabla siguiente) que, en este caso, corresponder a Enterprise Plus con encriptación de 40 bits.
El termino 120-3t es, obviamente, la versión (en este caso 12.0(3)T).
La m señala que el software se ejecutará desde la memoria RAM.

La z quiere decir que el archivo está zipeado o comprimido (un archivo comprimido se denota con una l), y debe descomprimirse al formato ejecutable .bin antes de poder descargarlo en el dispositivo en cuestión.

A continuación se presenta una tabla que contiene el código y conjunto de características:

Código	**Conjunto de características**
I	Solo IP
IS	IP Plus
D	Desktop
DS	Desktop Plus
J	Enterprise
JS	Enterprise Plus
AJ	Enterprise/APPN
AJS	Enterprise/APPN Plus
P	Proveedor de servicios
G	RDSI
C	Servidor de comunicación
F	CURAD
FIN	LANFRAD
B	Apple Talk
N	IP/IPX
R	IBM
F	Frame Relay
A	APPN (IBM)

Tabla A-3.2 Caractarísticas por código

Acontinuación se muestra la configuración completa de nombres de archivos.

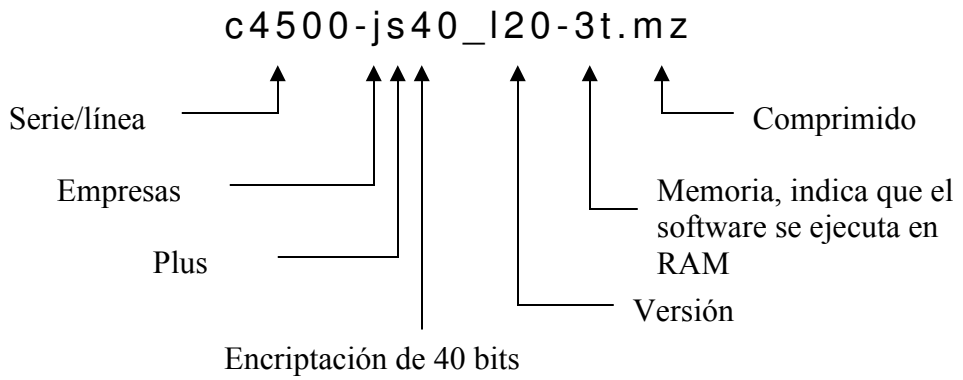


Figura A-3.2 Significado de cada uno de los términos que componen el nombre de un archivo de IOS de Cisco.

Arranque de un dispositivo Cisco.

Arrancar un dispisitivo Cisco es bastante fácil. Basta con activar la alimetación y darle al interruptor. Sin embargo, bajo esta sencilla operación suceden muchas cosas, que hay que conocer para el caso de que surjan problemas.

Lo primero qye ha de saberse es que el dispositivo efectúa una secuencia de prueba de arranque , de manera muy similar a un PC. Sin embargo, los equipos de Cisco no tienen códigos sonoros (bips), sino mensajes luminosos. Cada linea de estos dispositivos muestra los códigos de error de formas un tanto diferentes, aunque todas tienen en común el uso de estos mensajes de destellos luminosos.

Estos fallos puedens ser avisados por medio de LED. Si algún componente del conmutador no funciona bien en la prueba de autroarranque, se encenderán uno o más LED con luces amarillas . El puerto cuyo indicador luminoso se activa indica el componente que ha fallado.

Por lo tanto debe de saberse que tipo de indicadores luminosos activa normalmente el dispositivo de Cisco cuando todo va bien. Si aparece una indicación lumínica diferente, el operador sabrá que algo no ha funcionado.

CISCO IOS SOFTWARE MAJOR RELEASE 12.4 [16]

Ventajas / Que hay de nuevo / Desventajas / Vulnerabilidades criticas / Que lo soporta.

Más funcionalidad, soporte fuerte a hardware, introduce mas de 700 nuevas características a lo largo del espectro de hardware de la industria desde la versión 12.3 con enfoques en seguridad, VOIP, Alta disponibilidad, Ruteo de IPS, QoS, Multicasting, Addressing, Movilidad de IPS, y mejoras en VPNs Multipunto dinámica.

Mejoras puntuales importantes incluyen:

- Mejoras al IOS de Firewall
- Control de acceso a redes.
- Primer Cisco IOS de IPS (Intrusion Prevention System) Detección y Prevención de intrusos.
- Acceso CLI basado en roles designados.
- Administrador de equipo que soporte voz
- Niveles de Servicio Acordados a nivel IP para VOIP
- Actualización “light” de Cisco IOS
- Stateful Failover de IPsec
- IP routing perimetral (edge) optimizado
- Sitio de origen EIGRP MPLS VPN PE-CE
- Unidad de soporte prefija EIGRP
- Soporte y filtrado de mapas de ruteo EIGRP
- AutoQoS para la empresa, con QoS predeterminado
- Estimación de consumo de ancho de banda

Equipos de Hardware que soportan la IOS 12.4

- Cisco Small Business 100 Series Routers
- Cisco MWR 1900 Series Routers
- Cisco EtherSwitch Service Modules
- VPN Acceleration Module 2+ (VAM2+)
- Cisco 3200 Series Mobile Access Routers
- Cisco Gigabit Ethernet High-Speed WAN Interface Cards
- High-Density Analog (FXS/DIDFXO) and Digital (BRI) Extension Module for Voice/Fax
- HWIC-4ESW and HWIC-9ESW 4-and 9-port 10/100 Ethernet switch for Cisco 2800 and 3800 series
- Cisco 1800 Series Integrated Services Routers
- Cisco 4-port 10/100BASE-T
- Fast Ethernet Switch WAN Interface Card
- Cisco 1711 and Cisco 1712 Security Access Routers
- AIM-CUE Advanced Integrated Module
- Cisco 2800 Series Integrated Services Routers
- Cisco 3800 Series Integrated
- Services Routers
- Cisco Intrusion Detection System (IDS) Network Module
- IP Communications Voice/Fax Network Module
- 16- and 36-Port Ethernet Switch Module for Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series
- Cisco IAD2430 Series IOS Reduced IP subset/Voice
- 100BASE-FX SMF Network Module
- Cisco 1701 ADSL Broadband Router

Dentro de las diversas características, se prepara completamente para un entorno de sistemas completo. Equipos de Routers integrados cisco modelo 1800, 2800 y 3800. Primer sistema hardware/Software que integra servicios concurrentes a "wirespeed" velocidad alambrica que permite a los usuarios utilizar el router adecuado para cada punto remoto/oficina, mantener la red auto-defendida y además tener capacidad para ruteo avanzado de la red.

Es bastante escalonable desde pequeñas a grandes organizaciones ya que ofrece lo siguiente:

- Cisco 1800 con Data y Seguridad integrada
- Cisco 2800 con lo anterior más servicios avanzados de seguridad, data en voz y video.
- Cisco 3800 con lo anterior, más una gran densidad de servicios concurrentes.

Dentro de las ventajas claves están:

- Seguridad de voz integrada: encripción rápida, integración total con servicios de misión crítica.
- Mejor rendimiento (performance): nuevo diseño ASIC, el cual incrementa densidad, rendimiento de servicios, utiliza mejor los diversos servicios y memoria, aprovecha inteligencia y automatización.
- Más modular: hasta 2.2 GPS en los slots, alta densidad, módulos con form factor más grandes.
- Protección de la inversión: aprovecha los módulos existentes, hasta 4X de capacidad de memoria.

A continuación se describen aspectos relevantes de la IOS 12.4:

Disponibilidad para todos:

- Routers Cisco 830 ofrecen una pequeña opción de seguridad avanzada para voz, data, y video orientado a oficinas remotas pequeñas y usuarios remotos (tele-usuarios) que necesitan conectividad pero con seguridad.

- Muchas aplicaciones de QoS par aplicaciones y permite un uso e instalación fácil y administración remota sencilla con el Software IOS.

- Incluye VPN con protocolos como 3DES e Ipsec; además cuenta con un nuevo Cisco Easy VPN remote/server

- Soporta V3PN, que permite hacer uso de voz y video de manera sergura, QoS y multicast.

- Es bastante manejable, escalonable, y confiable: con el Cisco SDM, el CRWS (web setup del cisco router) e integración con IP solution center.

Seguridad

- Ofrece VPN multipunto dinámica, esto proporciona completa conectividad y una facilidad en la configuración de equipo. Permite aprovechar el ancho de banda ya que minimiza la latencia.

- Soporte de “spokes” dinámicos y adición de nuevos “spokes” en el DMVPN automática. Funcionalidad de DMVPN spoke-a-spoke, mejora el DMVPN al habilitar el intercambio seguro de data entre dos puntos remotos.

- Beneficios: creación inteligente de túneles a través de Internet, mejor

rendimiento al reducir congestionamiento de oficina principal, encripción y desencripción simplificada, previene duplicación de encripción/desencripción al hacer conexión directa entre oficinas.

- Posee certificación ICSA a nivel de Firewall.

- Aplicación de Firewall: avanzada inspección y control que incluye revisión de http o puerto 80, el cual es inspeccionado y se converge con el Software IOS Firewall con el nuevo IPS que controla las aplicaciones que esconden tráfico dentro del protocolo http como Messenger y kazaa. Administra consumo de ancho de banda basado en políticas.

- Motores de inspección de correo: controla uso inapropiado de protocolos de correo, escanea SMTP, IMAP, ESMTP y POP.

IOS para IPv6 permite al usuario implementar IOS firewall en IPv4 y IPv6 con los siguientes beneficios:

- Inspección de paquetes a nivel de protocolos TCP, UDP e ICMP.

- Soporte tanto de IPv4 e IPv6.

- Inspección de tráfico, previene de ataques que de otra manera se aprovecharían de fragmentos dentro de IPv4 e IPv6.

- Servicio de traslado de IPva aIPv6.

NAC (Network Admission Control)

- Utiliza inteligencia propia para detectar y limitar acceso a la red de puntos finales peligrosos. Viene incorporado “bundles” de seguridad de los 1800, 2800 y 3800.

- Además soporta múltiples productores de AntiVirus, entre ellos Trend Micro, McAfee, Symantec, IBM, etc.

Cisco IOS IPS (Intrusion Prevention System)

- Pioneros en cuanto a incorporar un IPS en un router.

- El IPS permite bloquear paquetes, resetear conexiones y generar alarmas.

- Soporta amplio espectro de ataques (740+), dinámicamente carga las firmas de ataques al router, integra tecnología de la familia Cisco IDS Sensor (los IDS 4200 appliance, catalyst 6500 IDS module y NM-CIDS).

Cisco AutoSecure

- Deshabilita servicios no-esenciales, elimina ataques DoS basados en falsos pedidos de servicios hechos al router.

- Refuerza lo relacionado al acceso seguro ya que proporciona mayor seguridad para acceder a los dispositivos, logs (bitácoras) mejoradas, previene que los atacantes sepan que los paquetes han sido botados.

- Asegura plano de reenvío (forwarding plane), protege contra ataques SYN, tiene anti-spoofing y refuerza la configuración stateful en imágenes externas del Firewall.

Rollback y Logging del AutoSecure

- Proporciona método de restauración de configuración de sistema al mismo estado en que estaba previo a la ejecución inicial del propio Cisco AutoSecure. Simplifica rastreo de la ejecución del comando AutoSecure,

inicializa "un-toque" lockdown del aparato con toda la confianza.

Controla "Plane Policing"

- Políticas de QoS que el usuario-define manejan y protegen con plano de control contra de ataques de reconocimiento y también ataques DoS.

- Durante un ataque el plano de control "ayuda" a sostener el tráfico con destino u origen del mismo plano durante un ataque.

- Se simplifica la configuración de políticas por el soporte CLI al QoS Modular; que minimiza la curva de aprendizaje, la cantidad de errores de provisionamiento y el propio tiempo y costo de definir e implementar políticas de QoS.

Acceso CLI role-based (basado en roles)

- Acceso a los comandos CLI son view-based (oh sea son capacidad de tener un set de comandos y configuraciones operacionales.

- Autenticación de usuarios se hace por medio de un Server AAA o TACACS+ ya sea externo o interno.

- El cliente puede definir hasta 15 vistas (views) mas una reserva, para el usuario raíz (root user).

Beneficios del Acceso CLI

- Seguridad: mejora la seguridad del aparato al definir el set de comandos CLI que son accesibles determinado usuario en particular.

- Disponibilidad: evita ejecución intencional de comandos CLI por personas no-autorizadas.

- Eficiencia Operacional: mejora el propio uso al prohibir que los usuarios vean

los comandos CLI que son inaccesibles a ellos.

Cisco Security Device Manager (CSDM o Cisco SDM)

Es una herramienta intuitiva basada en la Web, que simplifica la configuración del router y la seguridad con ayudantes inteligentes.

Beneficios de Cisco SDM

- Reduce tiempo de implementación con el ayudante WAN/VPN.

- Reduce el TCO al incluir nuevos atributos y mejoras del Cisco IOS sin mayor necesidad de capacitar a los encargados; esto lleva a que la administración sea más sencilla y menos costosa.

- Establece una política de seguridad consistente a lo largo de todos los routers y además de tener capacidades para hacer auditorias de seguridad.

- Auditoria de seguridad: tiene una configuración que es recomendada por ICSA y TAC.

- Ayudantes inteligentes: auto detectan errores de configuración y propone soluciones alternativas al error.

- Implementación rápida ya que posee un VPN Wizard que facilita la creación de VPNs.

- Herramientas para usuarios expertos: Editor ACL, monitoreo de túneles VPN.

Callmanager Express

Sistema integrado de voz y datos hecho para menos de 100 estaciones, con configuración flexible usando CLI o GUI Web, provee ayuda para hacer actualización a un hardware CCM centralizado. A prueba de lo que pueda traer el futuro en cuanto a arquitectura IP, por ejemplo, contenidos, QoS, Cisco IOS, VPN, DSL Ethernet y XML.

Agregar Unity Express hace una solución todo-en-uno.

Un hardware hecho para administrar todo lo relacionado a voz, puede ser negociado directo con el proveedor de servicio de enlaces. Es flexible para permitir adiciones como seguridad y aceleración de aplicaciones.

Control de Admisión de Red (Network Admision Control) [17]

Descripción

La infección de virus en redes de datos se ha convertido en un problema cada vez más serio. Los recursos consumidos durante un proceso de desinfección son mucho mayores que los recursos necesarios para implementear una solución de Antivirus en la red, tal es el caso de NAC o Control de Admisión de Red.

NAC es una iniciativa patrocinada por Cisco System. NAC utiliza la infraestructura de la red para hacer cumplir ciertos parámetros relacionados con las Políticas de seguridad. Esto lo hace en todos los dispositivos que buscan tener acceso a una red externa, obteniendo con ello un limitado número de amenazas que se podrían sufrir tales como virus, gusanos y spyware.

Usando NAC, las organizaciones pueden proporcionar acceso de red a los dispositivos, los cuales hayan sido verificados de que cumplen con la política de seguridad establecida. A la vez NAC puede identificar los dispositivo que no cumplan con las normas establecidas y negarles el acceso, colocarlos en un área de cuarentena y restringiendo el acceso.

NAC es parte de una iniciativa para aumentar la inteligencia de la red y con ello permitir a la red identificar, prevenir y adaptarse automáticamente a las amenazas de la seguridad.

NAC ofrece los siguientes beneficios:

- **Cobertura de Control Comprensivo:** Cubre todos los métodos que los host utilizan para conectarse a la red. Incluye Wireless, router WAN links, acceso remoto con IPSec y dialup.

- **Solución a distintos Proveedores:** NAC es el resultado de la colaboración de distintos proveedores de seguridad, incluyendo Antivirus y otros líderes del mercado. Ver la lista de participantes que se muestra en la tabla A-3.3.

- **Extensión de tecnologías y estándares existentes:** NAC amplía el uso de los protocolos de comunicación y de las tecnologías existentes, tales como: Protocolo de Autenticación Extensible (Extensible Authentication Protocol - EAP), 802.1x y Servicios RADIUS.

- **Extensión de Inversiones existentes de redes y antivirus:** NAC combina inversiones existentes en infraestructura de red y povee una tecnología de seguridad para el control de admisión.

NAC es un programa estratégico en el cual Cisco comparte características de su tecnología con los participantes aprobados en dicho programa.

Listado de Algunos Participantes:

Compañía	Nombre del Producto y Versión
• AHNLAB	V3Pro2004 for NAC
• BELARC	BelManage 2005, BelSecure 2005
• BIGFIX	BigFix Enterprise Suite
• CAYMAS SYSTEM	Caymas Identity-Driven Access Gateways, Release 2.6
• CITADEL SECURITY SOFTWARE	Hercules Enterprise Vulnerability Management 4.0
• COMPUTER ASSOCIATES	eTrust AntiVirus, eTrust PestPatrol
• F-SECURE	F-Secure Anti-Virus Client Security 6.00
• IBM	Tivoli Security and Identity Management Product Suite
• INFOEXPRESS	CyberGatekeeper Server 3.1 & CyberGatekeeper Policy Manager 3.1
• MCAFEE	VirusScan 7.x and 8.0i
• PATCHLINK	PatchLink Update with PatchLink Quarantine for NAC
• SECURE ELEMENTS	Class 5 AVR
• SENFORCE	Senforce Endpoint Security Suite 3
• SYMANTEC	Symantec AntiVirus 9.0 & Symantec Client Security 2.0
• TREND MICRO	Trend Micro OfficeScan Corporate Edition 6.5
• WHOLESECURITY	Confidence Online Enterprise Edition v4

Tabla A-3.3 Listado de participantes de NAC

¿ Por qué es Importante NAC ?

Porque permite reducir el riesgo evitando que los host vulnerables obtengan acceso de red normal. NAC se asegura que todos los anfitriones se acoplen a las políticas y actualizaciones del antivirus y del Sistema Operativo. De no cumplirse los requerimientos no se permitirá el acceso, reduciendo con esto ser blanco de posibles infecciones.

NAC es una tecnología que trabaja en conjunción con el Software Antivirus, determinando la condición de un host, antes de conceder acceso a la red. Esto asegura un sitio de trabajo tenga las firmas o actualizacioes necesarias y que no esté infectado antes de acceder a una red de datos.

Requerimientos de Sistema para NAC

Componente	Requerimientos Mínimos
Cisco IOS	IOS (12.3(8)T) o posterior (recomendada 12.3(8)T.1 O posterior)
Cisco Trust Agent	CTA 1.0 o posterior
Cisco Access Control Server	ACS 3.3 o posterior
Cisco Security Agent	CiscoWorks SIMS 3.1.2 o posterior
Trend Micro AV	Trend OfficeScan Enterprise 6.5
McAfee AV	McAffe VirusScan Enterprise 7.0, 7.1 y 8.0 i
Symantec AV	Symantec AntiVirus 9.0 y SCS 2.0 (Enterprise Developer Alliance Program)

Tabla A-3.4 Requerimientos para NAC (Sistema)

Plataformas que soportan Cisco NAC

Plataforma	Modelos	IOS
Cisco 7XXX	7200	IP IPSec 3DES IP FW/IDS IP FW/IDS IPSec 3DES Enterprise IPSec 3DES Enterprise FW/IDS Enterprise FW/IDS IPSec 3DES
Cisco 37XX	3745,3725	Advanced Security Advanced Services Advanced Enterprise
Cisco 36XX	3640/3640ª 3669-ENT Series	ENTERPRISE/FW/IDS PLUS IPSEC 3DES IP/FW/IDS IP/FW/IDS PLUS IPSEC 3DES IP/IPX/APPLETALK PLUS FW/IDS
Cisco 26XX	2600XM, 2691	Advanced Security Advanced Services Advanced Enterprise
Cisco 17XX	1701, 1711, 1712, 1721 1751, 1751-V, 1760	IP/ADSL/IPX/AT/IBM/VOX/FW/IDS Plus IPSec 3DES IP/ADSL/IPX/AT/IBM/FW/IDS Plus IPSec 3DES IP/ADSL/VOX/FW/IDS Plus IPSec 3DES IP/ADSL/FW/IDS PLUS IPSec 3DES Advanced Security Advanced Services Advanced Enterprise
Cisco 83x	831, 836, 837	IP/Firewall/IPSec 3DES PLUS IP/Firewall/IPSec 3DES/ PLUS/dial backup

Tabla A-3.5 Diversas Plataformas de Cisco que Soportan NAC

Plataformas que NO soportan Cisco NAC

Plataforma	Modelos
Cisco 17XX	1750, 1720, 1710
Cisco 26XX	2600 non-XM models
Cisco 36XX	3620, 3660-CO series

Tabla A-3.6 Plataformas que No soportan NAC

¿ Qué diferencia NAC de otras Soluciones?

Debido a la amplitud e integración que proporciona NAC en la infraestructura de la red, provee diversas ventajas sobre tecnologías similares:

- *Soluciones NAC tipo Appliance y de Framework están disponibles hoy.* Actualmente ningun otro vendedor ofrece ambas soluciones.

- *Solo NAC ofrece Control de cobertura comprensivo.* NAC soporta routers, switches, VPN´s, wireless access points, controladores de LAN wireless. Es también la única solución que apoya escenarios complejos como por ejemplo telfonía IP.

- *NAC provee soluciones para manejar todo tipo de dispositivos; además es la única solución que permite una integración para lograr un máximo control.*

- *Los componentes de NAC Appliance son completamente interoperable con soluciones tipo Framework, proporcionando una trayectoria exelente para posibles clientes.*

VIRTUAL ROUTER REDUNDANCY PROTOCOL (VRRP) [22]

VRRP es un protocolo estándar descrito en RFC 3768, el cual asigna de manera dinámica posibles rutas, para lo cual se implementa un router virtual quién administra los accesos hacia el resto de routers que se encuentren en una red. El proceso que implica implementar VRRP provee un Failover dinámico garantizando redundancia en los momentos que pudiera fallar determinado dispositivo.

Una alternativa a los protocolos dinámicos es la configuración estática de un router por defecto del lado del cliente o host. Esto simplifica la configuración del lado del cliente, pero crea un solo punto de falla. Si el Gateway por defecto falla, la comunicación es limitada únicamente al segmento de red interno ocasionando un corte de comunicación hacia el resto de la red. VRRP ha sido designado para eliminar los puntos de fallas.

El protocolo VRRP puede ayudar con el problema de la configuración dinámica. Ya que permite activar un grupo de routers hacia un solo router virtual. Entonces la red puede ser configurada con un router virtual como Gateway por defecto, ya que este representa un grupo de routers.

VRRP provee una función similar al protocolo “Hot Standby Router Protocol (HSRP)” VRRP es soportado en las interfaces siguierntes: Ethernet, Fast Ethernet y Gigabit Ethernet; también en MPLS VPN´s y VLANs.

VRRP fue introducido por CISCO en su lanzamiento 12.0 (18) ST. Posteriormente los siguientes lanzamientos de IOS ya soportan el estándar VRRP:

- 12.0(22)S
- 12.2(13)T
- 12.2(14)S

Topología Básica

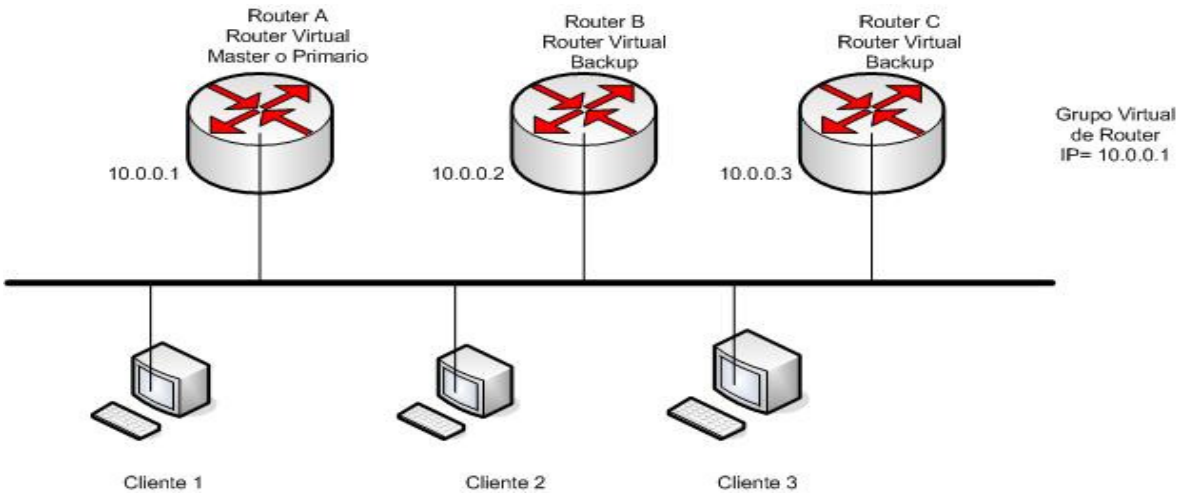


Figura A-3.3: Topología Básica utilizando VRRP. Se muestra una topología con VRRP configurado. En este ejemplo el Router A, B y C son routers VRRP que componen el router virtual. La dirección IP del router virtual es la misma que se configura en la interface del router A.

Topología VRRP de redundancia y carga compartida

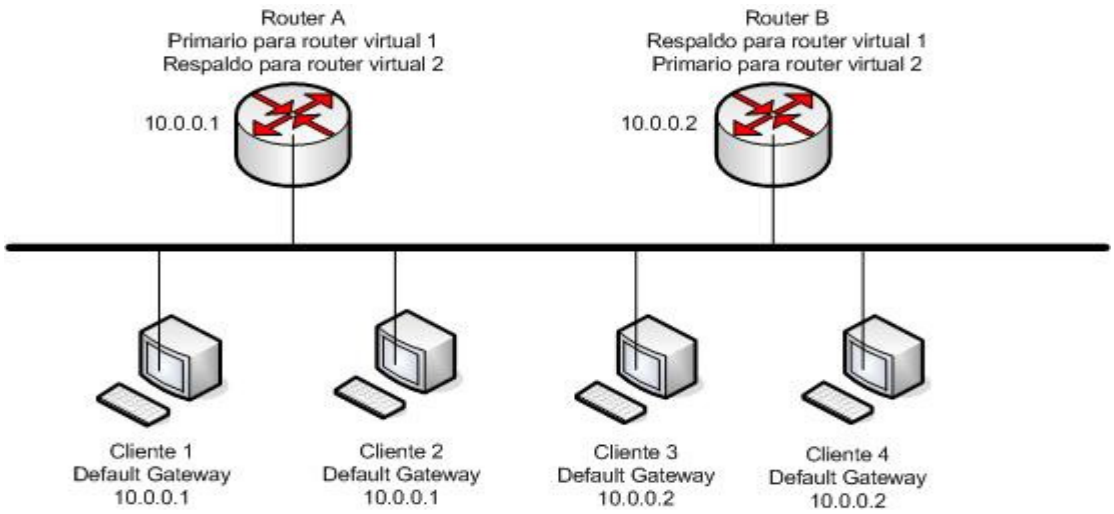


Figura A-3.4: En esta topología se muestran 2 router virtuales son configurados. Para el router virtual , router A es el propietario de la dirección IP 10.0.0.1 y es el configurado como primario; y router B es el router virtual de respaldo para el router A. Los clientes 1 y 2 han sido configurados con un Gateway por defecto con la IP 10.0.0.1. Para el router virtual 2, router B es el propietario de la IP 10.0.0.2 y es configurado como router virtual y router A es el respaldo del router B. Los clientes 3 y 4 han sido configurados con el gateway por defecto 10.0.0.2

Soporte de múltiples Routers Virtuales:

Se puede configurar arriba de 255 routers virtuales en una interface de router. Esto depende los siguientes factores:

- Capacidad de procesamiento del router
- Capacidad de memoria del router
- Que la interface del router soporte múltiples direcciones MAC

Prioridad usando VRRP:

Un aspecto importante en el esquema de redundancia VRRP es la prioridad del Router. La prioridad determina el rol de cada router VRRP y lo que pasa si el router primario virtual falla.

Si el router VRRP posee la dirección IP del router virtual y ésta dirección corresponde a la que tiene la interface física; se puede decir que el router funcionará como router virtual primario.
La prioridad también determina si la función del router es como router de respaldo. Se puede configurar la prioridad para cada router con los valores entre 1 y 254 usando el comando *vrrp priority*.

El router configurado como primario envía mensajes VRRP hacia otros routers del mismo grupo. Éstos comunican la prioridad y el estado del router primario. Estos mensajes son enviados por defecto cada segundo aunque puede ser configurable. Esto minimiza el tráfico en la red ya que únicamente el router primario envía periódicamente mensajes VRRP.

Beneficios de VRRP:

Redundancia: VRRP permite configurar múltiples routers como Gateway por defecto, reduciendo con esto la posibilidad de un punto de falla en la red.

Carga compartida: permite configurar VRRP de manera tal que el tráfico de la red pueda ser compartida por múltiples routers, haciendo que la carga de tráfico sea equitativa entre los routers disponibles.

Múltiples routers Virtuales: El router virtual puede administrar múltiples direcciones IP.

Autenticación: se puede asegurar que los mensajes VRRP que reciban de los routers sean autenticados configurandose con una contraseña.

Características Requeridas:

1. Respaldo de direcciones IP: esto es la función primaria del protocolo VRRP. Esto ayuda a:

- Minimiza la duración de los “Black Holes”
- Minimiza el gasto de ancho de banda.

- Función sobre una variedad de tecnologías de acceso múltiple que soporten tráfico IP.
- Provee la elección de múltiples routers en una red y permite el balance de cargas.
- Soporta múltiples subredes lógicas en un segmento de red.

2. Selección indicada de la trayectoria.
3. Minimización de interrupciones innecesarias del servicio.
4. Operación eficiente sobre redes extendidas.

Configuraciones de VRRP usando IOS Cisco:

El protocolo VRRP puede ser configurado de diversas maneras, para ello se definen 3 tareas de configuración:

- Personalizar VRRP
- Activar VRRP
- Verificar VRRP

Personalizando VRRP:

El modificar o personalizar VRRP es opcional. Para ello VRRP debe estar activado. Para modificar la configuración VRRP se pueden usar los siguientes comandos en modo de configuración de interface:

Comando	*Propósito o función*
Router(config-if)# vrrp group authentication string	Autentica paquetes VRRP provenientes de otros routers en un grupo determinado. Si se configura, todos los routers deben tener la misma cadena de autenticación.
Router(config-if)# vrrp group description text	Permite asignar una descripción a un grupo VRRP
Router(config-if)# vrrp group timers advertise [msec] interval	Permite configurar el intervalo de envío de mensajes VRRP por el router configurado como primario.
Router(config-if)# vrrp priority level	Permite establecer el nivel de prioridad. El número por defecto es 100
Router(config-if)# vrrp group timers learn	Permite configurar el router para que verifique los mensajes VRRP enviados por el router primario.

Tabla A-3.7: Commandos de personalizar VRRP

Activando VRRP:

Para activar VRRP se utilizan los siguientes comandos:

Comando	*Propósito o función*
Router(config)# interface type number	Configura la interface
Router(config-if)# vrrp group ipaddress	Activa VRRP en la interface e identifica la dirección IP primaria para router virtual.
Router(config-if)# vrrp group ipaddress secondary	Comando opcional y permite indicar una dirección IP adicional.

Tabla A-3.8: Comandos de activación de VRRP

Verificar VRRP:

Para verificar VRRP se pueden usar los siguientes comandos en modo EXEC:

Comando	*Propósito o función*

Router# show vrrp [brief | group]	Muestra un estado detallado de uno o varios grupos VRRP.
Router# show vrrp interface type number [brief]	Muestra los grupos VRRP y su estado en una interface específica

Tabla A-3.9: Commandos de verificación de VRRP

Comandos adicionales:

Los siguientes comandos permiten verificar o monitorear características en el momento que se ejecutan:

- *debug vrrp all*
- *debug vrrp error*
- *debug vrrp events*
- *debug vrrp packets*
- *debug vrrp state*

ANEXO 4.CONFIGURACIÓN BÁSICA DE UN DISPOSITIVO CISCO **[4]**

Una vez arrancado el dispositivo se puede empezar a configurar. En un equipo nuevo, la configuración suele realizarse mediante la conexión de la consola, porque el dispositivo todavía no tiene una dirección IP para configuración en Telnet. Sin embargo, después de iniciado el dispositivo merece la pena centrarse en una serie de detalles, que se muestran a continuacion (en lo sucesivo, los mensajes e indicaciones mostrados corresponderán al lOS estándar; la mayoría de estas indicaciones se han tomado de un enrutador de la serie 1750).

System Bootstrap, version 11.3(2)XA4, RELEASE SOFTWARE (fe1)
Copyright (e) 1999 by eiseo Systems, lne.
TAC:Home:SW:lOS:Speeials for info
C2600 platform with 32768 Kbytes of main memory

En esta sección hay dos puntos de la máxima importancia. Primero, se muestra la versión de arranque del sistema en el dispositivo. Se trata del mini-lOS que se está utilizando realmente para iniciar el dispositivo con la imagen lOS guardada en la memoria RAM flash. Podría interpretarse esta secuencia como la de un disco de arranque, con la salvedad de que normalmente se guarda en memoria ROM y por tanto, es difícil de cambiar. En segundo lugar, se muestra la cantidad de RAM del sistema instalada. Si este número no se corresponde con la que se sabe que está instalada, sería signo de que hay un problema en la instalación de dicha memoria RAM (la mayoría de los dispositivos de Cisco usan DRAM especial).

A continuación, se verá algo semejante a lo siguiente:

Program load complete, entry point: 0x80008000, size: 0x403b9c
Self descompressing the image :
##
################################## [OK]

Restrieted Rights Legend

Use, duplieation, or diselosure by the Government is

subjeet to restrietions as set forth in subparagraph

(c) of the Commercial Computer Software - Restricted

Rights elause at FAR see. 52.227-19 and subparagraph

(c) (1) (ii) of the Rights in Technical Data and Computer

Software clause at DFARS sec. 252.227-7013.

cisco Systems, lnc.

170 West Tasman Drive

San Jose, California 95134-1706

Cisco Internetwork Operation System Software

IOS (tm) C2600 Software (C2600 – I – M), Version 12.0(7)T,

RELEASE SOFTWARE (fc2)

Copyright (c) 1986-1999 by cisco system, lnc.

Compiled Tue 07-Dec-99 02:12 by phanguye

Image test-base: 0x80008088, data-base: 0x807AAF70

Hay también dos puntos de gran relevancia. El primero aparece en el párrafo que indica Self decompressing the image (autodescompresión de la imagen), seguido de una secuencia de símbolos # (algunos de los cuales se han omitido en este ejemplo) y al final, es de esperar que aparezca un OK. El enrutador descomprime la imagen si ésta está comprimida y puede auto descomprimirse, algo común en los enrutadores de las últimas generaciones. Esta característica permite ahorrar espacio en la preciada memoria RAM flash mediante la compresión de la imagen, que se descomprimirá completamente para su carga en RAM en el momento del arranque.
El segundo punto de interés se encuentra hacia el final de la serie de instrucciones. El mensaje lOS c2600 software indica qué versión de lOS se está cargando desde la RAM flash, con la cual se arrancará el dispositivo. En este caso, el enrutador 1750 está usando la versión l2.0(7)T.

Por último, en la siguiente pantalla aparece una información específica del hardware:

cisco 2611 (MPC860) processor (revision Ox203) with
26624K/6144K bytes of memory

Processor board ID JAD04360GH7 (4114038455)
M860 processor: part number O, mask 49
Bridging software.
X.25 software, Version 3.0.0.
2 Ethernet/IEEE 802.3 interface(s)
1 Serial network interface(s)
32K bytes of non-volatile configuration memory.
8192K bytes of proeesSOr board System flash (Read/Write)

Al principio de la misma puede verse el tipo de procesador y algunos datos sobre la RAM del equipo. En la sección que indica 26624K/6144K bytes of memory (26624K/6l44K bytes de memoria), el primer número es la cantidad de DRAM dedicada a la memoria principal (que se usa para ejecutar el lOS, el espacio de trabajo, etc.) y el segundo corresponde a la cantidad de memoria consagrada a la memoria compartida (que se usa como memorias intermedias en todas las interfaces). Estos dos números juntos deben sumar la cantidad total de DRAM del sistema. En algunos enrutadores, la proporción entre memoria principal y memoria compartida sigue una distribución fija, mientras que en otros es variable.

Seguidamente aparece algo de información sobre las características de software y las interfaces instaladas. Basta con cerciorarse de que los tipos de interfaz y las cuentas mostradas en la pantalla están de acuerdo con lo esperado. Después de las interfaces aparece la cantidad de memorias NVRAM y RAM flash instaladas.

En algunos dispositivos de Cisco (principalmente enrutadores), la primera pantalla que aparecerá ante el usuario será la llamada System Configuration Dialog (diálogo de configuración del sistema). Se trata en este caso de un asistente que guía al operador por toda la configuración inicial planteándole simplemente una serie de preguntas. Este proceso permite configurar el equipo incluso si no se tiene experiencia con la lOS. Seguidamente se revisan los mensajes que transmite el dispositivo y la explicación de lo que significan.
Después de pulsar la tecla ENTER se dará paso normalmente a la siguiente pantalla:

- System Configuration Dialog -
At any point you may enter a question mark '?' for help.
Refer to the 'Getting Started' Guide for additional help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
would you like to enter the initial configuration dialog? [yes]:

El [yes] significa que la respuesta por omisión a esta pregunta es «sí» y que bastaría con pulsar RETORNO para seleccionar esta opción. Eligiendo yes se accede al «asistente de configuración» (un término tomado de Microsoft, pero que aquí viene muy bien) denominado configuración básica de administración. En caso contrario, el sistema remitirá directamente a la interfaz de comandos en línea. No hay que preocuparse si se ha elegido no y se quiere acceder al asistente: bastará con reiniciar el dispositivo (ya que tiene una configuración de NVRAM o de arranque, aún en blanco) y se accederá a la misma petición. Alternativamente, puede introducirse el modo privilegiado o activar (que se verá más en profundidad cuando se hable de los modos lOS) y escribir setup para regresar a esta petición.
Además, puede pulsarse CTRL-C para salir completamente de lOS en cualquier momento, en caso de que se haya cometido algún error. Los cambios introducidos en la configuración no tendrán efecto hasta el final del proceso.
Suponiendo que se ha elegido yes, el siguiente mensaje en pantalla se parecería a lo siguiente:

First, would you like to see the current interface summary? [yes]:

Simplemente se pregunta si se desean ver las interfaces instaladas actualmente en el enrutador y los parámetros activos en dichas interfaces. Al elegir yes (sí) se accederá a la siguiente información:

Any interface listed with OK? value "NO" does not
have a val id configuration.
Interface IP-Address OK? Method Status protocol
TokenRing0 unassigned YES not set down down
Ethernet0 unassigned YES not set down down
Serial0 unassigned YES not set down down
Fddi0 unassigned YES not set down down
Como puede verse, en esta información se aportan algunos datos básicos:
¿Cuál es el nombre de la interfaz? .
¿Tiene una dirección IP asignada? .

¿Es funcional físicamente?.
¿Cómo se configuró la última vez?.
¿Está la interfaz activa? (en términos de Ethernet, ¿tiene un enlace?).
¿Hay protocolos activos en la interfaz?.

La mayoría de las veces lo único que interesará es que en esta página aparezcan todas las interfaces con las que se supone está instalado el enrutador. Como normalmente sólo se usa la herramienta de configuración cuando se instala el enrutador por primera vez, los valores de dirección IP, conjunto de métodos y otras informaciones se mostrarán en blanco. Si no aparece la interfaz, tal vez sea porque no funciona o posiblemente, porque en la lOS hay un error que hace imposible detectarla.

A continuación se presentará el mensaje siguiente:
Configuring global parameters:
Enter host name [Router]:

Aquí se escribe el nombre de anfitrión DNS deseado para el enrutador. Este nombre de anfitrión DNS se convertirá en el mensaje de petición a no ser que sea sobrescrito con el comando prompt.
El nombre de anfitrión DNS indica simplemente al enrutador cómo se llama.
Luego se verá el mensaje siguiente:

The enable secret is a password used to protect access to
privileged EXEC and configuration modes. This password, after entered, becomes encrypted in the configuration.

Enter enable secret:
The enable password is used when you do not specify an enable secret password, with some older software versions, and some boot images.
Enter enable password:

Las palabras clave enable secret y enable password se corresponden prácticamente con la contraseña del administrador en el dispositivo. Al activar el modo enable o privilegiado con la palabra clave secret o password se puede modificar la configuración y realizar diagnósticos que podrían interrumpir las operaciones del dispositivo. La diferencia entre estas dos palabras clave, secret y password, reside en que la primera está encriptada y no es visible en los archivos de configuración, mientras que la segunda aparece en texto sin encriptar. Cuando se configuran las dos se usa siempre secret, a no ser que se esté utilizando una versión antigua de lOS que no comprende la opción de activar contraseñas secreto.

Cuando se utiliza el modo de configuración, la lOS no permitirá definir estas dos contraseñas con el mismo contenido. Exigirá que sean diferentes

Después se obtendrá un mensaje como el siguiente:

The virtual terminal password is used to protect
access to the router over a network interface.
Enter virtual terminal password:

Ésta es la vty, o contraseña Telnet. Cada vez que el usuario intente acceder al enrutador desde Telnet, se le pedirá que introduzca esta contraseña, si está configurada.

Configure SNMP Network Management? [yes]:
Community string [public]:
Any interface listed with OK? value "NO" does not
have a valid configuration
Interface IP-Address OK? Method Status protocol
BRIO unassigned YES not set down down
Ethernet0 unassigned YES not set down down
Serial0 unassigned YES not set down down
Serial1 unassigned YES not set down down
Enter interface name used to connect to the
management network from the above interface summary: ethernet0

Aquí se permite configurar las funciones básicas SNMP en el enrutador, incluida la definición del nombre de comunidad y de la interfaz desde la que se administrará el enrutador. Seguidamente se obtendrá el mensaje:

Configure IP? [yes]:
Configure IGRP routing? [yes]:
Your IGRP autonomous system number [1]: 1

Esta petición permite activar IP en las interfaces. Como puede verse, las opciónes concretas aquí suministradas pueden variar según el modelo de enrutador utilizado y el conjunto de características del lOS. Puede pedirse al operador que configure IPX, DECnet, AppleTalk y otras pilas de protocolos siempre que el enrutador las admita. También se le instará a que configure los protocolos de enrutamiento. La siguiente pantalla mostrará lo siguiente:

Configuring interface parameters: Ethernet0
Configure IP on this interface? [yes]:
IP address for this interface: 192.168.1.1
Subnet mask for this interface [255.255.255.0]
Class C network is 192.168.1.0, 24 subnet bits; mask is /24

Aquí se puede realizar una configuración IP básica de todas las interfaces. De nuevo, las opciónes presentadas pueden variar según el modelo de enrutador y las interfaces instaladas. Finalmente, se construirá el archivo de configuración, que tendrá un aspecto similar a lo siguiente:

hostname enrutador
enab1e secret 5 1HNfx$Nhj5AqtXt823hCEBf.JZt. enable password test
line vty O 4
password open
snmp-server community public
!
ip routing

interface BRIO
no ip address

!
interface Ethernet0
ip address 192.168.1.1 255.255.255.0
!
interface Serial0
no ip address
!
interface Serial1
no ip address
!
router igrp 1
network 192.168.1.0
!
end

En estas líneas se detalla simplemente el formato de comandos 105 para todos los cambios solicitados. Después se pide al operador que guarde la configuración con la siguiente serie de opciónes:

[0] Go to the ros command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

La opción 0 sirve para volver a la IOS sin hacer ningún cambio. La 1 reinicia la configuración sin hacer cambios (útil cuando se ha cometido un error). La opción 2 guarda la configuración y vuelve al IOS, que es lo que normalmente se querrá hacer.
El inconveniente de este modo de configuración es que no permite configurar nada complejo o especial; y una vez que se conoce bien IOS, este modo resulta más largo y tedioso que simplemente escribir los comandos necesarios en la línea de la interfaz de usuario. Pero para principiantes ofrece una forma muy sencilla de lograr que el enrutador empiece a funcionar.

MODOS DE IOS

lOS se construye sobre varios modos de operación. Los modos principales se basan en niveles de privilegio. lOS incluye 16 niveles de privilegio, que van del 0 al 15; sin embargo, sólo 3 de ellos se usan por omisión. Los demás requieren el uso de una configuración especial.

EL NIVEL DE PRIVILEGIO 0

Se usa raramente. Los únicos comandos que se pueden activar en este nivel son help (ayuda), disable (desactivar), enable (activar), exit (salir) y logout (desconexión), lo que no le hace demasiado útil.

EL NIVEL DE PRIVILEGIO 1

Es el primer modo que se presentará después de conectarse al enrutador. Este modo se llama de privilegio de usuario, y a veces simplemente modo de usuario. En él no se pueden lanzar comandos dañinos para el dispositivo, es decir, no es posible emitir depuraciones (diagnóstico avanzado) ni ciertos comandos de

información (show), ni tampoco reconfigurar el dispositivo. Se usará este modo simplemente cuando se necesite información básica sobre el funcionamiento del dispositivo. Cuando se trabaje en modo de usuario, el símbolo de petición aparecerá del modo siguiente:

Router>

El símbolo mayor que (>) es la clave del modo en que se está. Si aparece, se estará trabajando en modo de usuario.

EL TERCER MODO DE OPERACIÓN

Es el de privilegio de sistema o, más brevemente, modo privilegiado o enable. Este modo tiene el nivel 15, y permite acceder a todos los comandos con que cuenta el dispositivo. Este modo se activa escribiendo enable, momento en el cual se pedirá al operador que introduzca una contraseña. Esta contraseña o palabra clave será la de tipo secret o de tipo password. Si se ha configurado una contraseña secret y el enrutador la ha aceptado, será ésta la que se use. En caso contrario, se utilizará el password.

Una vez activado con éxito el modo privilegiado, el símbolo de petición cambiará a la almohadilla (#), tal y como se ilustra seguidamente:

Router>enable password:
Router#

Desde este momento se puede emitir cualquier comando estándar, como los comandos show detallados y los comandos debug (comandos especiales de depuración utilizados para diagnóstico avanzado del sistema). También se pueden lanzar algunos comandos de configuración, como clear (borrar, para limpiar muchas cosas, desde el caché ARP a circuitos virtuales X.25), clock (reloj, para configurar la hora del sistema), reload (recargar, para reiniciar el dispositivo), copy (copiar, para copiar configuraciones e imágenes IOS) y erase (borrar, para suprimir imáge nes). Sin embargo, la mayor parte de las tareas de configuración se acometen en un cuarto modo:

EL MODO DE CONFIGURACIÓN

Para activar el modo de configuración desde el modo privilegiado se ha de escribir el comando configure (configurar) y luego especificar cómo se desea configurar el dispositivo. Por ejemplo, configure terminal significa que se va a configurar el dispositivo escribiendo los comandos de configuración manualmente. Éste es el método típico de configuración de dispositivos. Una vez arrancado el modo de configuración, los símbolos de petición vuelven a cambiar, como ilustra el ejemplo siguiente:

Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#

Este modo también se llama de configuración global, porque todos los comandos lanzados aquí afectan a la totalidad del dispositivo.

Un modo independiente, denominado de configuración de interfaz (aunque no siempre se trata de una interfaz), se usa para definir los parámetros específicos de una interfaz. Para acceder a este modo de configuración de interfaz se especifica qué interfaz se quiere configurar por medio del comando interface (interfaz), del modo siguiente:

Router(config)#interface Ethernet 0/0

Router(config-if)#

Como puede verse, el modo de configuración de interfaz no sólo es válido para interfaces. Se utiliza también para protocolos de enrutamiento, listas de acceso con nombre y otros comandos. Algunos de ellos se muestran en el siguiente ejemplo:

Router (config)# ip access-list Standard test
Router (config-std-nacl)#exit
Router (config)#router rip
Router (config-router)#exit
Router (config)#sub
Router (config)#suscribir-policy 1
Router (config-policy)#exit
Router (config)#

COMANDOS COMUNES DEL MODO DE USUARIO

A continuación se tratan los comandos comunes en el modo más elemental de funcionamiento de los dispositivos: el modo de usuario.
Hay que recordar que para saber en qué modo se está trabajando basta con mirar al símbolo de petición de la línea de interfaz de usuario. En esta línea, el indicador de modo de usuario aparecerá con un símbolo de «mayor que» (», en la forma: Router>. Los comandos tratados en este apartado son *connect* (conectar), *disconnect* (desconectar), *enable* (activar), *exit* (salir), *nameconnection* (nombre de conexión), *ping* (ping), *resume* (reanudar), *rlogin* (conexión remota), *show* (mostrar), *telnet, terminal* (terminal) y *traceroute* (camino de traza).

- Comando connect

El comando *connect* (conectar) se utiliza para establecer una sesión de terminal (Telnet) con otro dispositivo. En el modo de usuario este comando es idéntico al comando *telnet* y, en la práctica, para establecer una sesión Telnet no se necesita ninguna sesión Telnet. Para abrir una sesión Telnet, el método más sencillo consiste simplemente en teclear el nombre (si se ha configurado la tabla de anfitriones locales o de DNS) o la dirección IP del dispositivo remoto desde el símbolo de petición. El único caso en el que no es posible utilizar este método es cuando el nombre del dispositivo remoto es el mismo que el de un comando IOS (lo que sucede raras veces).

- Consideraciones especiales

En algunas situaciónes se puede desear mantener abiertas varias sesiones Telnet al mismo tiempo en el mismo enrutador. Esto se puede conseguir utilizando una combinación especial de teclas de comando para salir de las sesiones Telnet. Así, si se presiona CTRL-MAYÚSCULAS-6 y luego se teclea *x,* se «suspenderá» la sesión Telnet activa y se retornará al dispositivo anfitrión. Entonces se puede acceder por Telnet a otro dispositivo sin perder la primera conexión.

- Comando disconnect

El comando *disconnect* (desconectar) pone fin a una conexión Telnet. Este orden debe aplicarse en sesiones suspendidas, de manera que no es posible desconectar una sesión activa. En otras palabras, si se está conectado mediante Telnet a un enrutador, escribir *disconnect* no hará nada bueno (aunque si se teclea *exit* funcionará). Sin embargo, si se está en una conexión Telnet desde ese enrutador con otro enrutador y luego se suspende dicha sesión Telnet (CTRL-MAYÚSCULAS-6 x), se volverá al primer enrutador. Entonces, al escribir *disconnect* se pone fin a la conexión con el enrutador remoto.

Sintaxis

El comando *disconnect* básico desconecta la sesión utilizada más recientemente. También se puede usar el comando en la forma *disconnect [número de sesión]* para desconectar una sesión concreta.

- Comando enable

El comando *enable* (activar) simplemente aplica el modo de ejecución privilegiado (modo *enable)* al dispositivo.

Basta con escribir *enable* y usar la contraseña del acceso al modo privilegiado estándar. Opciónalmente se puede definir el nivel de privilegio para la conexión mediante el parámetro *enable;* pero a no ser que se hayan definido otros niveles de privilegio aparte del 1 y el 15, este comando no tendrá útilidad.

- Comando exit

El comando *exit* (salir) procede a una desconexión del dispositivo, cerrando cualquier sesión Telnet que se haya establecido y borrando la historia de comandos.

Sintaxis

Basta con escribir *exit.*

- Comando name-connection

El comando *name-connection* (nombre de conexión) permite asignar un nombre a una conexión Telnet suspendida. Mediante esta estrategia se hace más fácil recordar qué conexión corresponde a cada sesión, si bien lo normal es que cause más problemas que ventajas.

Sintaxis

Se debe de escribir *name-connection.* El enrutador preguntará el número de conexión al que se desea dar nombre, y luego qué nombre se le quiere poner. Una vez terminada la asignación del nombre a la conexión, pueden aplicarse los comandos de control de sesión (como *disconnect* y *resume)* en la sesión por nombre.

- Comando ping

Posiblemente uno de los comandos de prueba de conectividad más útiles es el universal *ping.* En lOS, *ping* funciona como en casi cualquier otro sistema operativo: envía paquetes de solicitud de eco del protocolo de mensajes de control de Internet (ICMP, *Internet Control Messaging Protocol)* y recibe respuestas de eco. Sin embargo, en lOS, *ping* puede aprovecharse más porque los códigos son un tanto singulares. En el modo de usuario se usa lo que se conoce como un ping estándar. Con un ping estándar puede especificarse sólo el anfitrión al que se envía el comando. El modo privilegiado incluye además un comando *ping* extendido, que permite especificar muchos más parámetros que una simple dirección IP. Por ahora, nos concentraremos en la versión del *ping* correspondiente al modo de usuario

Cuando se envía un *ping* a otro dispositivo, se reciben códigos con los resultados.

Sintaxis

Basta con escribir *ping [dirección IP* / *nombre de anfitrión].*

Códigos ping

	Ping con éxito
	Sin respuesta
U	Destino inaccesible (inaccesible «genérico»)
N	Red inaccesible
P	Puerto inaccesible
Q	Recibida la disminución del tráfico desde el origen
M	Paquete inaccesible debido a un bit DF (no se puede fragmentar el paquete para envío)
¿	Paquete desconocido recibido como respuesta

Tabla A-4.1 Códigos de Ping

El comando *resume* (reanudar) reanuda una sesión Telnet suspendida anteriormente.

Sintaxis

Se escribe *resume* y el nombre (si se ha configurado con el comando *name-connection)* o el número de la sesión, del modo: *resume [nombre / número].* También se puede escribir *resume* para reanudar la última conexión activa.

Comando rlogin

El comando *rlogin* (conexión remota) permite conectarse con un sistema UNIX remoto utilizando el protocolo rlogin. El comando *rlogin* es parecido a *telnet,* con la salvedad de que se ha de especificar un nombre de usuario cuando se inicia la conexión.

Sintaxis

El comando se utiliza escribiendo *rlogin [dirección IP /nombre de anfitrión].* Opciónalmente, pueden usarse también las opciónes *-l nombre usuario* o */user nom-breusuario* para especificar el nombre de usuario para rlogin. Ambas opciónes tienen la misma función, pero la *-l* es la sintaxis UNIX y la */user* corresponde a la sintaxis lOS estándar. lOS admite ambas. Si no se especifica nombre de usuario, por defecto rlogin se aplica al nombre de usuario local. Las sesiones de rlogin también pueden suspenderse, reanudarse y desconectarse de igual modo que las Telnet.

- Comando show

El comando *show* (mostrar) es posiblemente el más utilizado de lOS. Es el principal comando de visualización y mediante su uso puede inspeccionarse casi cualquier parte de un componente lOS. Al ser *show* un comando tan versátil y extenso.

Sintaxis

Primero se menciona la sintaxis estándar empleada por todos los comandos *show* y luego se entrara en detalle en cada una de las formas individuales del *show.* La sintaxis del comando *show* estándar es *show [parámetro] [modificadores].* El campo parámetro especifica el comando *show* individual de que se trate, como, por ejemplo, *show dock.* Los modificadores (que pueden ser varios) pueden apuntar al parámetro de modo más específico en el caso de un tema amplio (como *show ip route)* o concretar el detalle de la información recuperada (por ejemplo, *show ip interface brief).* Tal es la fórmula básica que suelen seguir todos los comandos *show.*

- Comando show aliases. El comando *show aliases* (mostrar alias) ofrece una lista de todos los alias del modo actual. Se llama *alias* a pseudocomandos que invocan comandos reales con apenas una o dos teclas. Por ejemplo, el alias por defecto de *show* es s. La sintaxis de este comando es *show aliases.* Opciónalmente, se puede añadir el modo al final del comando para ver los alias de un modo distinto a aquel en que se está en la actualidad. Por ejemplo, *show aliases exec* muestra todos los alias del modo privilegiado *(enable).*

- Comando show arp. El comando *show arp* (mostrar ARP) muestra la tabla del protocolo de resolución de direcciones (ARP, *Address Resolution Protocol)* para todo el dispositivo, con independencia de cuál sea el protocolo de capa superior (al contrario que *show ip arp,* por ejemplo, que muestra únicamente la tabla ARP para IP). La sintaxis de este comando es simplemente *show arp.*

- Comando show async. El comando *show async* (mostrar asíncrono) muestra la información relativa a las conexiones serie asíncronas. Tiene dos modificadores: *bootp* y *status.* El comando *show async bootp* muestra todos los datos extendidos (como información del archivo de arranque y direcciones del servidor de tiempo) enviados como respuesta a las peticiones *bootp.* Por su parte, el comando *show async status* obtiene las estadísticas de tráfico asíncrono, además de todas las co-

nexiones asíncronas actuales. Estos dos comandos son accesibles únicamente en el modo privilegiado.

- Comando show cdp. El comando *show cdp* se utiliza para ver todos los vecinos del protocolo de descubrimiento de Cisco (CDP, *Cisco Discovery Protocol)* conectados directamente, además de la información básica de configuración CDP. El comando *show cdp* muestra la configuración CDP y permite el uso de varios modificadores para mostrar informaciones más específicas, como se indica a continuación:

show cdp entry [nombre]. Muestra información detallada sobre los vecinos. Tiene los modificadores opciónales siguientes:

- *show cdp entry [nombre] protocolo* Muestra el direccionamiento de capa 3 de la entrada.
- *show cdp entry [nombre] version.* Muestra la versión lOS del dispositivo remoto.
- *show cdp interface [tipo de interfaz y número].* Muestra la configuración CDP de cada interfaz.

-*show cdp neighbors.* Muestra un resumen de todos los vecinos. Tiene los modificadores opciónales siguientes:

- *show cdp neighbors [tipo de interfaz].* Permite ver directamente los vecinos conectados directamente basándose en el tipo de conexión (Ethernet, serie, etc.).
- *show cdp neighbors detail.* Muestra información detallada (semejante al comando *show cdp entry)* de todos los vecinos.
- *show cdp traffic.* Muestra estadísticas de tráfico para CDP.

- Comando show clock. Este comando, como se habrá adivinado, muestra la hora y la fecha del enrutador. También muestra si se cree que la hora es correcta o no, de acuerdo con los ajustes de sincronización horaria del dispositivo.

- Comando show async. El comando *show async* (mostrar asíncrono) muestra la información relativa a las conexiones serie asíncronas. Tiene dos modificadores: *bootp* y *status.* El comando *show async bootp* muestra todos los datos extendidos (como información del archivo de arranque y direcciones del servidor de tiempo) enviados como respuesta a las peticiones *bootp.* Por su parte, el comando *show async status* obtiene las estadísticas de tráfico asíncrono, además de todas las conexiones asíncronas actuales. Estos dos comandos son accesibles únicamente en el modo privilegiado.

- Comando show debugging. *Debugging es* una forma de diagnóstico avanzado con la que puede verse información muy detallada sobre lo que ocurre dentro del dispositivo Cisco. El comando *show debugging* muestra qué elementos han de depurarse en un momento dado. Este comando es algo útil cuando se está realizando una búsqueda de errores en un sistema que ya ha sido revisado por alguna otra persona; nunca sabe qué depuraciones puede haber realizado ya esa persona.

- Comando show dhcp. Este comando se utiliza principalmente en conexiones RDSI o serie que utilizan protocolo punto a punto (PPP, *Point-to-Point Protocol).* Muestra información de asignación de direcciones IP y de servidores conocidos de protocolo de configuración dinámica de anfitrión (DHCP, *Dynamic Host Configuration Protocol) o* La forma *show dhcp lease* de este comando muestra información sobre todas las asignaciones DHCP en todas las interfaces. Por su parte, el *show dhcp server* muestra todos los servidores DHCP conocidos y las estadísticas sobre las asignaciones dadas y liberadas.

- Comando show diag. El uso principal del comando *show diag* es mostrar información de diagnóstico sobre los módulos instalados en un enrutador. Aunque gran parte de la información revelada en su resultado es de útilidad sólo para ingenieros de Cisco, en parte puede resultar también enormemente valiosa para los

administradores de redes (como sucede con las descripciones detalladas, incluyendo números de modelo, de los módulos y tarjetas instalados). La sintaxis de este comando es *show diag [número de ranura].* Si se escribe sólo *show diag,* se obtendrá toda la información disponible sobre todas las ranuras.

- Comando show flash. Este comando puede mostrar información detallada no sólo sobre el contenido del sistema de archivos de memoria flash y la cantidad de espacio libre, sino también sobre cuántas ranuras SIMM/DIMM flash están en uso. La forma más aprovechable del comando es *show flash: al/,* que muestra toda la información disponible de la memoria flash.

- Comando show history. El comando *show history* (mostrar historia) muestra simplemente los comandos lanzados desde la conexión al enrutador, o hasta el máximo configurado para el tamaño de la memoria búfer de historia. Este comando no tiene modificadores.

- Comando show hosts. El comando *show hosts* (mostrar anfitriones) muestra una tabla de anfitriones, junto con el dominio por defecto y el método de búsqueda (estático o DNS) para el enrutador. La sintaxis del comando es *show hosts [modificador]* y el único modificador es un nombre opciónal (en caso de que se desee buscar una entrada en particular).

- Comando show interfaces. El comando *show interfaces* (mostrar interfaces) es uno de los más utilizados de esta clase. Su cometido consiste en suministrar información sobre interfaces individuales en el sistema que es independiente del protocolo (capa 3 y superiores). El comando se utiliza principalmente en la forma *show interfaces,* que muestra información detallada sobre todas las interfaces del

sistema y también en la forma *show interface [tipo y número de interfaz],* que muestra información detallada sobre una interfaz específica. Existen otras opciónes y modificadores para ver las propiedades de gestión de colas y puentes, aunque dependen no sólo del tipo de interfaz, sino también del tipo y el modelo del dispositivo.

- Comando show ip. El *show ip* (mostrar ip) es más un conjunto de subcomandos que un comando en sí mismo. Al constar de un número tan amplio de subcomandos (más de 50 en algunos enrutadores), a continuación se explican únicamente los que se utilizan con más frecuencia.

show iparp. Similar al comando *show arp,* con la salvedad de que en este caso sólo se muestra la tabla ARP para IP.

show ip interface. Similar al comando *show interface,* excepto porque muestra información detallada específica de IP sobre las interfaces. La forma básica de este comando, *show ip interface,* muestra los detalles sobre todas las interfaces del enrutador. La forma abreviada del comando, *show ip interface brief,* muestra información resumida sobre todas las interfaces.
Finalmente, la forma *show ip interface [nombre y número de interfaz]* muestra información detallada sobre una interfaz en concreto.

show ip sockets. Muestra los sockets abiertos en el enrutador.

show ip traffic. Muestra estadística detallada sobre el protocolo de Internet (IP, *Internet Protocol);* el protocolo de mensajes de control de Internet (ICMP, *Control*

Messaging Protocol), y el tráfico multidifusión en el enrutador, e incluyen estadísticas de difusiones y errores.

ANEXO 5. PROTOCOLO RIP **[4]**

RIP es un protocolo de enrutamiento de vectores de distancia destinado a redes redundantes pequeñas y medianas. Se trata de un producto que no depende del fabricante y su versión 1 se define fundamentalmente en RFC 1058. Esta independencia del fabricante proporciona al protocolo RIP la ventaja de que pueden manejarlo múltiples fabricantes simultáneamente (incluso Microsoft lo admite, en caso de que fuera necesario utilizar un elemento de Windows 2000 como enrutador). Al tratarse de un protocolo tan sencillo, también resulta muy fácil de configurar. Desafortunadamente, su simplicidad lo hace más vulnerable a una serie de problemas.

FUNCIONAMIENTO BÁSICO DEL PROTOCOLO RIP

El funcionamiento básico del protocolo RIP es muy sencillo y tiene en cuenta ciertas normas elementales:

Cuando un enrutador se inicializa, las únicas rutas de las que tiene constancia son las redes a las que está directamente conectado.
En la versión 1 del protocolo RIP, el enrutador transmite información sobre todas las redes conocidas a todas las redes directamente conectadas. Estas difusiones se conocen como actualizaciónes o anuncios.
Los enrutadores RIP «escuchan» las difusiones RIP. De esta manera, pueden informarse sobre las redes de las que no tengan constancia directamente.
La métrica utilizada en el protocolo RIP se basa en el número de saltos (que puede definirse como el número de enrutadores presentes en la ruta) y se anuncia en las difusiones RIP que se efectúan a cada red. El número máximo de saltos en RIP es de 15. Una métrica de 16 se considera infinita.

Se supone que cualquier ruta que conozca un enrutador RIP pasa por dicho enrutador. En otras palabras, si el Enrutador A envía una actualización al Enrutador B, este último supone que el salto siguiente correspondiente a las redes que se incluyen en la actualización es el Enrutador A.

Las actualizaciónes se envían en intervalos regulares.

Para comprender más a fondo el funcionamiento de este protocolo hay que conocer unas cuantas características adicionales: los relojes de actualización, el horizonte dividido (con o sin envenenamiento inverso), los relojes de espera, el envenenamiento de ruta y las actualizaciónes provocadas.

Los relojes de actualización sirven para que el enrutador sepa cuánto debe esperar antes de enviar actualizaciónes periódicas. En la versión 1 del protocolo RIP, cada actualización incluye todas las rutas (salvo las que haya eliminado el horizonte dividido), independientemente de si se han producido cambios desde la última actualización. El proceso periódico de actualización garantiza que los enrutadores puedan determinar si otros enrutadores están apagados. Sin embargo, el breve periodo de tiempo que el protocolo RIP espera entre dos actualizaciónes, junto con el hecho de que en cada actualización se anuncia toda la tabla de enrutamiento, indica que las actualizaciónes de este protocolo pueden utilizar buena parte del ancho de banda en redes complejas. El reloj de actualización se puede configurar en los enrutadores de Cisco, pero hay que garantizar que todos los enrutadores tengan las mismas configuraciones de reloj.

El horizonte dividido es una de las númerosas características implementadas en el enrutamiento de vectores de distancia para reducir la aparición de bucles de enrutamiento. El horizonte dividido básico garantiza que las rutas comunicadas a través de una interfaz dada nunca se difundan desde la misma interfaz. Además, la red relacionada con una interfaz nunca se anuncia en ella. El horizonte dividido con envenenamiento inverso reduce el tiempo de convergencia que se asocia a esta característica, en caso de que se produzca un bucle de enrutamiento mediante el anuncio de una métrica infinita en una interfaz dada para las rutas difundidas a través de dicha interfaz.

Por su parte, los relojes de espera sirven para evitar los bucles en una topología compleja, al solicitar que el enrutador RIP espere un periodo de tiempo específico (por omisión, 180 segundos, o seis veces el intervalo de actualización) antes de considerar verdadera cualquier información sobre una ruta actualizada. Los relojes

de espera resultan similares a las verificaciones de la realidad propias del enrutamiento de vectores de distancia.

El envenenamiento de ruta se usa para reducir la aparición de bucles de enrutamiento. Sin él se eliminan las entradas incorrectas de enrutamiento de la tabla después de que caducan el tiempo muerto de la ruta y los relojes de eliminación de ruta. El reloj de tiempo muerto de ruta (denominado reloj inválido en IOS) se usa para determinar cuándo ha fallado una ruta. Si una actualización no ha oído acerca de una ruta dada antes de que este reloj caduque, dicha ruta se considera no válida y entra en fase de espera. Sin embargo, sigue siendo utilizada (pero ya no se anuncia) hasta que caduca el reloj de eliminación de ruta. Cuando caduca este reloj, se elimina por completo la ruta de la tabla de enrutamiento.
La configuración por omisión para el tiempo muerto de ruta es de 180 segundos, mientras que la del reloj de eliminación de ruta es de 240 segundos. Sin el envenenamiento de ruta, un enrutador simplemente deja de anunciar rutas inadecuadas cuando caduca el reloj de tiempo muerto de la ruta. De esta manera, el enrutador siguiente de la fila tiene que esperar a que caduque el tiempo muerto de su ruta, y así sucesivamente. Esto significa que en una red RIP grande (de más de diez saltos) podrían transcurrir más de treinta minutos hasta que todos los enrutadores tuviesen noticia de la existencia de una ruta inadecuada (lo que puede hacer innecesarios los relojes de espera). El envenenamiento de ruta funciona con las actualizaciónes provocadas para reducir este tiempo, anunciando una ruta con una métrica infinita (de 16 en RIP) una vez que caduca el tiempo muerto de su enrutador. Cuando se combina el envenenamiento de ruta con las actualizaciónes provocadas, éste podría reducir el tiempo de convergencia para una red de más de diez saltos a menos de 30 segundos.

Las actualizaciónes provocadas sirven para reducir la posible aparición de bucles de enrutamiento y el tiempo de convergencia de la red. Si falla un enlace a una red directamente conectada, en lugar de esperar a que caduque un reloj de actualización, el protocolo RIP anuncia el fallo inmediatamente (como una distancia infinita, igual que ocurre con el envenenamiento de ruta). De la misma manera, una vez que se ha actualizado una ruta, el protocolo RIP anuncia a continuación la ruta actualizada, en lugar de esperar a que caduque el reloj de actualización. Finalmente, si se produce un fallo indirecto (por ejemplo, que el enrutador no se percate de la existencia de una ruta anunciada y que el reloj de tiempo muerto caduque), las actualizaciónes provocadas se usan conjuntamente con el envenenamiento de ruta para propagar rápidamente el fallo de ruta en cuestión.

En este punto puede parecer que el protocolo RIP ya no es tan sencillo como se anunciaba. Sin embargo, es realmente un protocolo muy simple. La simplicidad tiene sus ventajas, pero el mayor inconveniente de este protocolo está en los bucles de enrutamiento. Estos últimos hacen necesarias todas estas características adicionales que complican la cuestión.

CARACTERÍSTICAS DEL PROTOCOLO RIP1

A continuación se señalan otras características más avanzadas del protocolo RIP1. En primer lugar, se analiza la cualidad de este protocolo para añadir más de una ruta a la tabla de enrutamiento y efectuar el balance de cargas.

Por omisión, los enrutadores de Cisco usan hasta cuatro rutas de coste equivalente y aplican el balance de cargas entre ellas. Con el protocolo RIP, si un enrutador recibe información sobre una ruta dirigida a una red por parte de dos o más enrutadores y todas las rutas están empleando la misma métrica, el enrutador llevará a cabo un balance de cargas de coste equivalente entre todas las rutas.

El cuello de botella se produce cuando un enrutador no está enterado de que existe una diferencia de velocidad entre dos rutas. Este problema se presenta con mayor frecuencia en el protocolo RIP, ya que este protocolo no tiene forma de especificar la velocidad de los enlaces (su métrica sólo se ocupa de establecer el número de

saltos). Sin embargo, este problema también puede aflorar en otros protocolos (generalmente, debido a una configuración inadecuada).
La única manera de asegurar que no se produzca un cuello de botella es garantizar que todos los enlaces redundantes de métrica equivalente tengan el mismo ancho de banda.

Otro inconveniente que presenta la versión 1 del protocolo RIP es su imposibilidad de enviar máscaras con actualizaciónes de enrutamiento. Como resultado, no se puede utilizar la versión 1 del protocolo RIP en redes basadas en complejos sistemas de subredes VLSM o CIDR. Teniendo en cuenta que la versión 1 del protocolo RIP no envía máscaras con sus actualizaciónes, tiene que presuponer que se está usando cierta máscara cuando recibe una actualización. Las reglas básicas que el protocolo RIP aplica a las actualizaciónes recibidas son las siguientes:
Si la actualización que introduce una interfaz comparte la misma clase de red que cualquiera de las direcciones IP de la interfaz del enrutador, el protocolo RIP aplica la máscara usada en la interfaz correspondiente a la actualización. Si después de aplicar la máscara de la interfaz a la actualización se establecen los bits de la misma en la parte del servidor, el protocolo RIP inserta la ruta en la tabla con una máscara de 32 bits (255.255.255.255), lo que significa que la ruta es para un servidor individual.
Si la actualización que introduce una interfaz no comparte la misma clase de red que el resto de las direcciones IP de la interfaz del enrutador, el protocolo RIP aplica, por omisión, la máscara de clase A, B o C a dicha actualización.
Las reglas que sigue el protocolo RIP para las actualizaciónes enviadas son las siguientes:

Si durante el envío de una actualización desde una interfaz, la dirección de red de clase A, B o C de la dirección IP aplicada a dicha interfaz es la misma que la dirección de red de clase A, B o C de las entradas de ruta presentes en la actualización y la máscara aplicada a la interfaz que realiza el envío es la misma que la utilizada para las subredes de la actualización, el protocolo RIP transmite los números de subred de la actualización, pero no envía las máscaras.

Si durante el envío de una actualización desde una interfaz, la dirección de red de clase A, B o C de la dirección IP aplicada a dicha interfaz es la misma que la dirección de red de clase A, B o C de las entradas de ruta presentes en la actualización y la máscara aplicada a la interfaz que realiza el envío es diferente de la máscara utilizada para las subredes de la actualización, el protocolo RIP no envía la actualización.
Si durante el envío de una actualización desde una interfaz, la dirección de red de clase A, B o C de la dirección IP aplicada a dicha interfaz es diferente de la dirección de red de clase A, B o C de las entradas de ruta presentes en la actualización, el protocolo RIP hace un resumen de la ruta como la que va dirigida a toda la clase de redes A, B o C.

Para facilitar las cosas, la solución más sencilla al hecho de no incluir máscaras de subred en la actualización es utilizar la misma máscara para todas las subredes de una red con una clase A, B o C dada, o bien emplear un protocolo de enrutamiento (como la versión 2 del protocolo RIP o EIGRP) que soporte VLSM.

VENTAJAS Y DESVENTAJAS DE LA VERSIÓN 1 DEL PROTOCOLO RIP

Ventajas	Desventajas
Es muy fácil de entender y configurar.	Es ineficaz (ocupa demasiado ancho de banda).
Está admitido casi con seguridad por todos los enrutadores.	Convergencia lenta en redes grandes.
Admite el balance de cargas.	Sólo admite balance de cargas de coste equivalente. El cuello de botella puede ser un obstáculo.
Generalmente está libre de bucles.	Generalmente está libre de bucles.
	Escalabilidad limitada (máximo de 15 saltos).
	No tiene en cuenta el ancho de banda, el retardo ni la fiabilidad a la hora de aplicar la métrica.
	No soporta VLSM.
	Si una red es grande, compleja y dada a los cambios, es posible que los enrutadores nunca converjan del todo.
	Las actualizaciónes difundidas pueden provocar un derroche masivo de ciclos de UPC en los servidores.
	No admite actualizaciónes autenticadas, lo que significa que un enrutador molesto podría perturbar el funcionamiento de las rutas.

Tabla A-5.1 Ventajas y Desventajas de RIP

Está claro que las desventajas del protocolo RIP superan con mucho a sus ventajas. Ahora cabría preguntarse por qué utilizar el protocolo RIP si es tan problemático. Muchos expertos se han planteado esta misma cuestión durante mucho tiempo, pero lo cierto es que es un protocolo fácil de configurar y goza siempre de soporte. No obstante, prácticamente en todos los casos resulta recomendable el EIGRP frente al RIP (si se utilizan enrutadores de Cisco) o el OSPF (si se emplean otros enrutadores). En otras palabras, suponiendo que realmente se necesitara un protocolo de enrutamiento dinámico.

En muchos casos, el protocolo RIP se usa simplemente porque los administradores que han participado en la implementación de la red no comprenden el enrutamiento lo suficiente como para añadir las rutas estáticas correctas. Para ellos es más sencillo dejar que el protocolo RIP lo haga automáticamente. Si es el caso, conviene volver a plantearse el protocolo RIP. En la mayoría de los casos, si se trabaja en una escala lo suficientemente pequeña como para usar el protocolo RIP, tal vez convenga utilizar en su lugar enrutamiento estático.

MEJORAS QUE INTRODUCE EL PROTOCOLO RIP 2

La versión 2 del protocolo RIP (definido fundamentalmente en RFC 2453) supera algunas deficiencias de la versión 1 sin que esto suponga un cambio drástico de protocolo. En el listado siguiente se detallan las mejoras más útiles de la versión 2:

Soporte VLSM. Las máscaras de subred se transmiten con las actualizaciónes del protocolo RIP 2.

Actualizaciónes multidifundidas. Las actualizaciónes se transmiten mediante multidifusión en lugar de utilizar la difusión normal, ahorrando así el número de ciclos de UPC a los servidores no RIP.

Soporte de autenticación. Se admite la autenticación de texto no cifrado para los enrutadores compatibles con RFC (los enrutadores de Cisco también admiten la autenticación cifrada en MD5).

La versión 2 sigue presentando muchos de los inconvenientes de la versión 1, pero también conserva las ventajas que supone su simplicidad y su soporte prácticamente unánime. Si hay que usar el protocolo RIP, la versión 2 suele ser la mejor elección.

CONFIGURACIÓN BÁSICA DEL ROUTER RIP

Afortunadamente, la configuración del protocolo RIP es muy sencilla. Para configurarlo utilizando las opciónes por omisión basta con emplear dos comandos: router rip y network [dirección de red].

Cuando se introduce el comando router rip desde el modo de configuración global, se activa el protocolo RIP de forma global y se sitúa en el modo de configuración de enrutador, como se ilustra a continuación:

Router(config)#router rip
Router(config-router)#

Una vez en el modo de configuración del enrutador, se pueden introducir los comandos de red para activar de forma individual el enrutamiento RIP para cada red basada en clases. Hay que destacar que el comando network lleva a cabo las tres funciones siguientes:

Anuncia las rutas pertenecientes a la red específica basada en clases.
Se escuchan todas las actualizaciónes en todas las interfaces pertenecientes a la red basada en clases en cuestión.
Se envían actualizaciónes en todas las interfaces pertenecientes a la red basada en clases en cuestión.

En el momento de introducir el comando network para una red dada se activan estas tres funciones. Es una situación de todo o nada, imposible de controlar selectivamente. También hay que advertir que el comando activa las tres funciones en relación con toda una red basada en clases.

Finalmente, si se desea modificar la versión del protocolo RIP que se está utilizando, basta con usar el comando version [1 | 2] o ip rip [send version l receive version] [1 l 2]. El comando version se introduce desde el modo de configuración

de enrutador y se establece la versión del protocolo RIP utilizado en el enrutador de forma global. Si se desea cambiar la versión del protocolo RIP para enviar o recibir actualizaciónes en una interfaz dada (por ejemplo, cuando ésta está conectada a un enrutador que sólo admite el protocolo RIP 1, pero el resto del entorno admite el protocolo RIP 2), hay que usar el comando ip rip. El ejemplo siguiente muestra cómo configurar la versión en 1 para todas las actualizaciónes enviadas fuera de la primera interfaz Fast Ethernet:

Router(config)#interface fastEthernet %
Router(config-if)#ip rip send version 10

CONFIGURACIÓN AVANZADA Y OPTIMIZACIÓN DEL PROTOCOLO RIP

En un enrutador de Cisco se puede utilizar una serie de comandos opciónales para obtener un mayor control sobre el protocolo RIP. Aunque ninguno de estos comandos es necesario, pueden resultar muy útiles en ciertos casos. A continuación se especifican diversas tareas de configuración opciónales:

Configuración de interfaces pasivas (desactivando actualizaciónes difundidas).
Configuración de actualizaciónes unidifusión.
Incorporación de compensaciones métricas a las rutas.
Ajuste de los relojes RIP.
Desactivación del horizonte dividido.
Establecimiento del número máximo de rutas.
Configuración de la autenticación (RIP 2).
Desactivación de autorresumen (RIP 2).

CONFIGURACIÓN DE INTERFACES PASIVAS

Una interfaz pasiva es una interfaz que no difunde actualizaciónes de enrutamiento, pero que sigue anunciándose en dichas actualizaciónes y también sigue escuchando cuando éstas aparecen. Si se recuerdan las tres tareas que realiza el comando network (anuncia todas las redes presentes en la red basada en clases, escucha las actualizaciónes en todas las interfaces presentes en dicha red y difunde actualizaciónes en todas las interfaces de la misma), el comando passive interface suspende la tercera tarea realizada en una interfaz en particular. Esta función resulta especialmente útil en dos situaciónes comunes:

Cuando la red vinculada a la interfaz RIP sólo incluye servidores, pero debe ser anunciada a otros enrutadores.
Cuando por razones de seguridad o rendimiento conviene desactivar las actualizaciónes de enrutamiento difundidas y elegir selectivamente los enrutadores que recibirán actualizaciónes unidifusion.

El comando passive interface tiene la siguiente sintaxis: passive-interface [tipo y número de interfaz]. Se introduce el comando desde el modo de configuración de enrutador, como se muestra a continuacion:

Router(config)#router rip
Router(config-router)# network
Router(config-router)# passive-interface Ethernet %

CONFIGURACIÓN DE LAS ACTUALIZACIONES DE UNIDIFUSIÓN

Aunque el protocolo RIP 1 suele usar difusiones para las actualizaciónes de enrutamiento y el protocolo RIP 2 usa en su lugar multidifusiones, en ciertas situaciónes puede resultar necesario activar actualizaciónes unidifusión. Es en estos casos cuando se envían actualizaciónes a través de un enlace que no admite difusiones (como es el caso de las redes NBMA), como el Frame Relay. También resultan útiles cuando no se desea que las difusiones derrochen recursos de UPC en clientes

vinculados a la misma red, como el enrutador que requiere el envío de difusiones. Finalmente, las actualizaciónes unidifusión son útiles en situaciónes en las que se busca seguridad entre varios enrutadores para las actualizaciónes de enrutamiento. Como las actualizaciónes para cada enrutador son unidifusión, en una red conmutada, los servidores normales no podrían utilizar un rastreador para leer los detalles de cada actualización RIP.

Para activar las actualizaciónes unidifusión hay que usar el comando de modo de configuración de enrutador neighbor [dirección ip]. Para el ejemplo anterior, la configuración de Flagg es la siguiente:

Router (config)# router rip
Router (config-router)# network
Router (config-router)# neighbor
Router (config-router)# passive-interface Ethernet 0/0

¿CÓMO AÑADIR UNA COMPENSACIÓN MÉTRICA?

Añadir una compensación métrica a una ruta permite especificar que la métrica asignada a las rutas procedentes de un enrutador o red dados aumente una cantidad específica. Esta funcionalidad permite especificar de un modo rudimentario que las rutas procedentes de uno o más enrutadores sean menos favorecidas que otras.
Para añadir una compensación métrica se usa el comando offset-list [(opciónal) lista de acceso] [in I out] [offset] [(opciónal) tipo y número de interfaz].
La sección [(opciónal) lista de acceso] es un componente opciónal que se puede utilizar para añadir una compensación a las entradas de actualización que concuerden con la lista de acceso.

La configuración necesaria aparece en el código siguiente:
Router (config)# router rip
Router (config-router)# network
Router (config-router)# offset-list in 5 Ethernet 0/0

AJUSTE DE LOS RELOJES DEL PROTOCOLO RIP

Ajustar los relojes del protocolo RIP resulta útil si se desea optimizar la convergencia de la red. Por ejemplo, en una red interna de alta velocidad y ancho de banda considerable (como una LAN de Fast Ethernet), tal vez se desee reducir el valor de los relojes, permitiendo que RIP converja más rápidamente a costa del ancho de banda. Sin embargo, en una WAN tal vez se prefiera aumentar el valor de los relojes para reducir el uso del ancho de banda, sacrificando el tiempo de convergencia. De una u otra manera, cuando se modifican los relojes, no hay que olvidar que se deben configurar todos los enrutadores para que usen los mismos valores de reloj, así como recordar las relaciones que establecen los relojes entre sí. Para simplificar este proceso, en la tabla siguiente aparecen los múltiplos de reloj recomendados.

Reloj	**Multiplo**	**Tiempo por omission (IP RIP)**
De actualización	Reloj Base	30 segundos
No Valido	3 veces el de actualización	180 segundos
De espera	3 veces el de actualización	180 segundos
Eliminación de ruta	Mayor que el no valido	240 segundos

Tabla A-5.2 Ajsutes de reloj del Protocolo RIP

Si se tienen muchas rutas, configurar los relojes en un valor poco elevado puede hacer que el procesador de alto nivel use los enrutadores. El valor por omisión de 30 segundos para el reloj de actualización es adecuado para la mayoría de los enlaces WAN y puesto que la convergencia no suele plantear ningún problema en las LAN (ya que deberían tener configuraciones más o menos estáticas, lo que haría que fallaran muy rara vez), mantener los relojes en su valor por omisión es lo correcto en muchas situaciónes. Sin embargo, si la red cambia a menudo (generalmente debido a fallos de enlace), la disminución de los valores de reloj puede acelerar la convergencia.

Para establecer los valores de los relojes del protocolo RIP, hay que usar el comando de modo de configuración de enrutador timers basic [tiempo de actualización en segundos] [tiempo de invalidez en segundos] [tiempo de espera en segundos] [tiempo de eliminación de la ruta en segundos]. Por ejemplo, para asignar al reloj de

actualización un valor de 15 segundos, al reloj no válido 45 segundos, al reloj de espera 55 y al reloj de eliminación de la ruta 100, habría que ejecutar el comando siguiente:

Router (config-router)# timers basic 15 45 55 100

Esta configuración hace que el enrutador envíe y espere recibir actualizaciónes cada 15 segundos, que declare una ruta inadecuada tras 45 segundos sin actualización y entre en fase de espera, que permanezca en dicha fase unos 55 segundos adicionales y luego, 100 segundos mas tarde, proceda a eliminar la ruta de la tabla.

IMPLEMENTACION DE TÉCNICAS DE FILTRADO

CONFIGURACIÓN DE LAS ACL

El primer paso a la hora de configurar las ACL consiste en comprender la sintaxis de las listas de acceso. En el caso de una lista de acceso estándar, la sintaxis no resulta demasiado compleja. Sin embargo, en el caso de las listas de acceso extendidas, la sintaxis puede resultar un poco más confusa. En la siguiente tabla se describen las características de los comandos para la creación de ACL.

Comando	Descripción	Modo
Access-list [número de lista de acceso] [deny \ permit] [origen] [mascara comodin de origen] [log]	Crea una lista de acceso IP numerada de carácter estándar.	Configuración Global
Access-list [número de lista de acceso] [deny \ permit] [protocolo] [origen] [mascara wilcard de origen] [operadores de puerto (opciónales)] [destino] [mascara wilcard de destino] [operadores de puerto (opciónales)] [established] [log] ip access-list estándar [nombre]	Crea una lista de acceso numerada de carácter extendido	Configuración Global
Access-list [nombre]	Crea una lista de acceso numerada de carácter estándar	Configuración Global
[deny \ permit] [origen] [mascara wilcard de origen] [log]	Introduce sentencias en una lista de acceso IP denominada de carácter estándar	Configuración de lista de acceso
Ip access-list extended [nombre]	Crea una lista de acceso IP denominada de carácter extendido	Configuración Global

Tabla A-5.3 Muestra pámetros de construcción ALC

[deny \ permit] [protocolo] [origen] [mascara wilcard de origen] [operadores de puerto (opciónales)] [destino] [mascara wilcard de destino] [operadores de puerto (opciónales)] [established] [log]	Introduce sentencias en una lista de acceso IP denominada de carácter extendido	Configuración de listas de acceso
ip access-group [número o nombre de lista de acceso] [in \ out]	Aplica una lista de acceso a una interfaz	Configuración de Interfaz
Show ip access-list [número o nombre de lista de acceso]	Muestra una o todas las listas de acceso IP	Ejecución de usuario
Show access-list [número o nombre de lista de acceso]	Muestra una o todas las listas de acceso	Ejecución de usuario

Tabla A-5.4 Muestra pámetros de construcción ALC

El primer comando que aparece en la lista *access-list*, se usa para crear listas de acceso IP numeradas de carácter estándar y extendido. El factor decisivo que indica si una lista de acceso debe ser estándar o extendida es simplemente el número utilizado para definir la lista de acceso. Si dicho número está comprendido entre 1 y 99, la lista de acceso será una ACL IP estándar. Si, por el contrario, el número utilizado se sitúa entre 100 y 199, la lista de acceso será una ACL IP extendida
En las nuevas versiones del IOS, las ACL numeradas con valores comprendidos entre 1300 y 1999 también están disponibles para las ACL IP estándar.

La configuración de las listas de acceso en el formato numerado sigue una serie de reglas de carácter simple:

Las listas de acceso coinciden con las sentencias introducidas utilizando comandos de lista de acceso múltiples con el mismo número, para crear listas multisentencia.
Las listas de acceso coinciden con las sentencias procesadas en el orden introducido, donde la primera sentencia coincide con el paquete que se está utilizando.

Se incluye una sentencia *deny* al final de cada ACL, lo que significa que una vez que se aplica a una interfaz, todos los paquetes que no coincidan con cualquiera de las sentencias *permit* presentes en una ACL se abandonarán automáticamente.
Las sentencias individuales presentes en las listas de acceso numeradas no pueden modificarse. Para eliminar una sentencia ACL hay que utilizar el comando *no access-list [número]*, eliminando todas las sentencias asociadas con dicha ACL.

A continuación se explica cómo se construye una lista de acceso IP numerada estándar.

LISTAS DE ACCESO ESTÁNDAR

La sintaxis utilizada para el comando *access-list* cuando se construye un listado estándar resulta muy sencilla:
"access-list [número de lista de acceso] [deny I permit] [origen] [máscara wilcard de origen] [conectar]"

El número debe situarse, lógicamente, en el rango que va de 1 a 99. La sección *deny I permit* especifica la acción que se efectuará (denegar o permitir) en relación con los paquetes que cumplen esta sentencia. Las secciones origen y máscara wilcard de origen definen qué paquetes deben coincidir, basándose en la dirección de origen, y el parámetro opciónal log indica al IOS que conecte con paquetes que coincidan con esta lista de acceso con la función syslog.

Las únicas partes de una lista de acceso IP estándar que generan cierta dificultad son las secciones de dirección de origen y la de máscara wildcard. La sección origen es la parte de la dirección de origen con la que se desea coincidir. Por ejemplo, si se desea coincidir con todas las direcciones de origen en la red 172.16.0.0, habría que introducir 172.16.0.0 como dirección de origen. Verdaderamente, se puede colocar cualquier cosa que se desee en los últimos octetos de la dirección (siempre y cuando se configure la máscara correctamente), pero no tiene sentido introducir una

dirección completa cuando lo único que se desea es efectuar una coincidencia con los primeros dos octetos.

La máscara realmente determina qué cantidad de la dirección de origen forma parte de la coincidencia. La máscara está escrita en el formato wildcard (comodín), y quizás pueda parecer que está colocada en orden inverso a cómo cabría esperar. En una máscara wilcard, las partes de la dirección que se describen mediante el valor binario 0 en la máscara deben coincidir exactamente, mientras que se ignoran las partes que tienen un valor binario 1.

Por ejemplo, para efectuar una coincidencia con 172.16.0.0-172.16.255.255, habría que introducir la dirección de origen de 172.16.0.0 con una máscara wilcard de 0.0.255.255. Siguiendo la misma lógica, para efectuar una coincidencia con cada dirección IP situada entre 192.168.1.128 y 192.168.1.255 habría que introducir una dirección de origen de 192.168.1.128 con una máscara wilcard de 0.0.0.127.

Esta combinación coincide con las direcciones IP seleccionadas, ya que en lenguaje binario todos los bits que tienen un valor 0 deben coincidir con la IP de origen escogida (192.168.1.128), mientras que todos los valores binarios 1 pueden ser diferentes.

Basándose en esta información, si se desea configurar un filtro de paquete utilizando ACL estándar para bloquear todas las transmisiones desde 192.168.1.1, autorizar todas las comunicaciones desde el resto de la red 192.168.1.0 y denegar todas las demás, habría que crear el filtro de paquete con los comandos siguientes:

Router(config)#access-list 1 deny 192.168.1.1 0.0.0.0
Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255

Para especificar un anfitrión individual hay que utilizar la palabra clave *host* en la ACL. Por ejemplo, en el comando anterior, en lugar de escribir *access-list 1 deny 192.168.1.10.0.0.0*, habría que escribir *typed access-list 1 deny host 192.168.1.1.*

Para garantizar la creación de esta lista de acceso se pueden utilizar los comandos *show ip access-list* o *show access-lists*.

Ejemplo:

Router# show access-lists
Standard IP access list 1deny 192.168.1.1permit 192.168.1.0, wildcard bits 0.0.0.255
Router# show ip access-list
Standard IP access list 1 deny 192.168.1.1 permit 192.168.1.0, wi1dcard bits 0.0.0.255

El orden de los comandos en una ACL resulta muy importante. Por ejemplo, si se reorganizan estas sentencias, la dirección 192.168.1.1 tendría autorización para comunicarse, ya que dicha dirección coincide con 192.168.1.00.0.0.255. Hay que recordar que una ACL simplemente utiliza la primera sentencia coincidente e ignora el resto.

Por lo general, lo lógico es colocar las entradas más específicas en la parte superior de la lista. El truco consiste en examinar mentalmente el orden de la lista, punto por punto, y garantizar que todos los objetivos se encuentren satisfechos en el listado. Sin embargo, a medida que la lista se complica, este proceso se hace cada vez más complejo.

Por ejemplo, hay que suponer que se desea configurar un listado que efectúe las siguientes tareas:
Autorizar todas las direcciones situadas en el rango que va de 192.168.1.64 a 192.168.1.127.

Autorizar las que van de 192.168.1.1 a 192.168.1.3.
Autorizar todas las direcciones comprendidas entre 10.0.2.0 y 10.255.255.255.
Denegar todas las demás direcciones.

En este caso, se podría utilizar la siguiente lista de acceso para cumplir estas metas:

Router(config)#access-1ist 1 permit 10.0.0.0 0.255.255.255
Router(config)#access-1ist 1 permit 192.168.1.64 0.0.0.127
Router(config)#access-1ist 1 permit host 192.168.1.1
Router(config)#access-1ist 1 permit host 192.168.1.2
Router(config)#access-1ist 1 deny 10.0.1.0 0.0.0.255

Es necesario reconocer los problemas que surgen con esta lista. A continuación se examinará cada objetivo en orden para garantizar el análisis de cada uno de los problemas.

En primer lugar, se desea autorizar el rango que va de 192.168.1.64 a 127. Mirando en la lista, la segunda sentencia cumple este objetivo. Sin embargo, la sentencia access-list 1 permit 192.168.1.64 0.0.0.127 coincide con todas las direcciones IP situadas entre 192.168.1.0 y 192.168.1.127.
El segundo objetivo consiste en autorizar el rango que va desde 192.168.1.1 hasta 192.168.1.3 para establecer la comunicación. Aunque la tercera, la cuarta y la quinta sentencia efectúan esta tarea, ésta no es la manera más eficaz de hacerla. Además, la segunda sentencia del listado se alcanzaría antes de acceder a estas sentencias.

El tercer objetivo consiste en autorizar todas las direcciones situadas en el rango que va de 10.0.2.0 a 10.255.255.255 para establecer la comunicación. Aunque la primera sentencia, access-list 1 permit 10.0.0.0 0.255.255.255, cumple esta tarea, coincide con todas las direcciones desde la red 10.0.0.0.
El objetivo final es denegar todos los paquetes, lo cual no se lleva a cabo debido a las siguientes razones:

La segunda sentencia autoriza al rango que va de 192.168.1.0 a 192.168.1.63 para que establezcan la comunicación.

La primera sentencia autoriza todas las direcciones de la red 10.0.0.0 (10.0.0.0 a 10.255.255.255) para que establezcan la comunicación, lo cual no coincide con el rango especificado.
Para eliminar estos problemas habría que reconstruir la lista de la siguiente manera:

Router(config)#access-1ist 1 deny 10.0.0.0 0.0.1.255
Router(config)#access-1ist 1 permit 10.0.0.0 0.255.255.255
Router(config)#access-1ist 1 permit 192.168.1.64 0.0.0.63
Router(config)#access-1ist 1 permit 192.168.1.0 0.0.0.3

Hay que observar que, en este caso, se puede realizar esta tarea con sólo cuatro sentencias. La primera sentencia deniega el rango de dirección IP que va de 10.0.0.0 a 10.0.1.255.

La segunda sentencia autoriza todas las direcciones de la red 10.0.0.0 que no coincidan con la primera sentencia. La tercera sentencia admite todos los paquetes situados en el rango que va de 192.168.1.64 a 192.168.1.127.

La cuarta sentencia autoriza todos los paquetes que van de 192.168.1.1 a 192.168.1.3.

Una vez creada la lista de acceso, será preciso aplicarla a una interfaz y elegir una dirección utilizando el comando *ip access-group [número o nombre de lista de acceso] [entradalsalida].* Hay que recordar que cuando se aplica una lista de acceso se suele desear hacerlo tan cerca del origen del paquete como sea posible. De esta manera, si se desea utilizar esta lista para realizar una coincidencia interna con los usuarios que entren en el enrutador, habría que aplicar la lista a la interfaz de enrutador interna con la dirección entrante, como se muestra a continuación:

Router(config-if)# ip access-group 1 in

Hay que tener en cuenta que sólo se puede aplicar una lista de acceso individual en cualquier interfaz para el tráfico orientado hacia dentro o hacia fuera (una ACL por dirección). Por tanto, es preciso garantizar que todas las metas requeridas puedan alcanzarse con una ACL individual.

En el caso de una lista de acceso nombrada, el proceso es casi idéntico, exceptuando el hecho de que se modifica la ACL. Cuando se introduce la ACL se emplea el comando ip access-list standard [nombre]. Este comando permite cambiar al modo de configuración de lista de acceso para la lista de acceso nombrada, como se ilustra a continuación.

Router(config)#ip access-1ist standard test
Router(config-std-nac1)#

Una vez en el modo de configuración de lista de acceso se pueden introducir los parámetros de lista de acceso utilizando sentencias *permit o deny*

Router(config-std-nac1)# deny 10.0.0.0 0.0.255.255
Router(config-std-nac1)# permit 172.16.0 0.0.255.255

Estas sentencias se procesan en el orden en que se introduzcan, como ocurre con las listas de acceso numeradas. La única diferencia está en el hecho de que, a diferencia de las listas de acceso numeradas, se pueden eliminar comandos individuales en una lista de acceso nombrada mediante el uso de sentencias específicas *no deny o no permit*.

La diferencia fundamental que existe entre una lista de acceso con nombre y una numerada radica en la capacidad de utilizar nombres descriptivos para listas de acceso con nombre y la capacidad de modificar entradas individuales en las listas de acceso numeradas. Sin embargo, esta última diferencia suele quedar anulada, ya que basta con copiar la sentencia de lista de acceso en el portapapeles desde una

lista de acceso numerada (mostrada en un comando show run o show star) y reordenar la lista a placer. Una vez terminado este proceso, basta con eliminar la lista de acceso original con un comando no *access-list [número]* y pegar la lista de acceso modificada en la ventana del terminal.

LISTAS DE ACCESO EXTENDIDAS

Después de conocer las ACL estándar, se explicarán las complejidades propias de las ACL extendidas. En una ACL extendida se pueden especificar muchos más parámetros, protocolos (incluyendo IP, TCP y UDP), direcciones de destino y puertos (para TCP y UDP).
Las ACL IP extendidas numeradas pueden utilizar rangos que van de 100 a 199 o de 2000 a 2699.
Con una ACL extendida se debe especificar un protocolo para generar la coincidencia. El protocolo con el que se establece dicha coincidencia puede ser cualquier número de protocolo IP situado entre 1 y 255, o cualquiera de las siguientes palabras clave:

IP (para coincidir con todos los paquetes IP).
ICMP
TCP
UDP
EIGRP
IGRP
OSPF

Cuando se genera una coincidencia con TCP o UDP se abren otras posibilidades interesantes. Se puede elegir la posibilidad de establecer coincidencias con
puertos de origen o de destino. Cuando se coincide con puertos es preciso tener la capacidad de efectuar la coincidencia basándose en cinco operadores:

lt. Menor que el número listado.

Gt. Mayor que el número listado.
Eq. Igual que el número listado.
Neq. Distinto del número listado.

También se pueden especificar puertos mediante el uso de palabras clave en lugar de números. Entre las palabras clave IOS reconocidas para puertos se incluyen las siguientes: BGP, ECHO, FINGER, FTP, FTP-DATA, GOPHER, NNTP, POP2, POP3, SMTP, SYSLOG, TELNET, WHOIS, Y WWW.

Asimismo, es posible especificar la autorización de paquetes (o su rechazo, aunque esto último no resulta útil) basándose en el paquete que forma parte de una sesión previamente establecida mediante el uso de la palabra clave "*established"*.

Para ver de qué forma casan todas estas piezas adicionales en una ACL extendida, a continuación se analizará un conjunto de metas de filtrado y se explicará cómo alcanzar estos objetivos. Las metas requeridas para filtrar los paquetes entrantes en la interfaz externa del enrutador se enumeran a continuación:
Deben autorizarse todos los paquetes destinados a 192.168.1.1 utilizando un puerto 80 de destino TCP.
Deben autorizarse todas las comunicaciones que se originen desde la red privada a los servidores web externos que útilicen HTTP y HTTPS.
Deben autorizarse todas las comunicaciones entrantes desde el anfitrión externo 10.1.1.1 que útilicen números de puerto de origen TCP y UDP que vayan de 22.000 a 44.000.
Deben autorizarse todas las comunicaciones entrantes al anfitrión 192.168.1.200.
Deben autorizarse todas las sesiones no establecidas que entren en la inter-faz externa y útilicen puertos de destino conocidos al anfitrion 192.168.1.100.
Debe rechazarse todo el tráfico restante.
Para alcanzar el primer objetivo hay que introducir una sentencia similar a la siguiente:

Router(config)#access-list 100 permit tcp any host 192.168.1.1 eq 80

La palabra clave *any* indica al enrutador que debe realizar una coincidencia con cualquier IP origen. Como el puerto no se especifica a continuación, se efectúa una coincidencia con todo. Para establecer una coincidencia en los puertos de origen.
La sección *host 192.168.1.1* indica al enrutador que debe efectuar una coincidencia con el anfitrión de destino 192.168.1.1. Finalmente, *eq 80* indica al enrutador que debe efectuar una coincidencia con el puerto destino 80. Este filtro efectúa exactamente la tarea requerida: establece coincidencia con todas las comunicaciones procedentes de cualquier anfitrión destinado a 192.168.1.1 utilizando el puerto de destino 80 TCP 80 (HTTP).

Segundo objetivo:

Router(config)#access-1ist 100 permit tcp any eq 80 any estab1ished
Router(config)#access-1ist 100 permit tcp any eq 443 any established

Como lo que se desea es autorizar exclusivamente los paquetes que útilicen HTTP o HTTPS para regresar a los anfitriones situados en la red interna, es necesario establecer una coincidencia con el puerto de origen en 80 y 443 en lugar de hacerlo con el de destino. Asimismo, puesto que únicamente se desea devolver paquetes procedentes exclusivamente de las sesiones previamente establecidas por estos anfitriones, se utiliza la palabra clave "*established*."

Para autorizar todas las comunicaciones entrantes procedentes del anfitrión externo 10.1.1.1 utilizando números de puerto de origen TCP y UDP comprendidos entre 22.000 y 44.000, hay que introducir dos sentencias similares a las siguientes:

Router(config)#access-1ist 100 permit tcp 10.1.1.1 range 22000 44000 any
Router(config)#access-1ist 100 permit udp 10.1.1.1 range 22000 44000 any

Para autorizar todas las conexiones internas al anfitrión 192.168.1.200 hay que utilizar la sentencia siguiente:

Router(config)#access-1ist 100 permit ip any host 192.168.1.200

Finalmente, para autorizar conexiones utilizando puertos de destino conocidos al anfitrión 192.168.1.100 hay que utilizar la sentencia siguiente:

Router(config)#access-list 100 permit ip any host 192.168.1.100 lt 1024

Una vez terminada la construcción de la ACL, cabe aplicarla a la interfaz externa del enrutador, utilizando el comando estándar *ip access-group [número o nombre de lista de acceso] [in I out].*

Las ACL extendidas con nombre siguen los mismos principios generales que las ACL numeradas, por lo que aquí no se analizarán sus características. Basta con aplicar los principios relacionados con las ACL extendidas a los comandos enumerados en el apartado dedicado a las ACL nombradas estándar.

FILTRADO DE URL

IMPLEMENTANDO FILTRO DE URL

Configurar filtro de URL es un proceso directo. Sin embargo, se puede querer instalar o habilitar opciónes de configuración. Se muestra la manera como se configura el router para que interactue con un producto de servidor de contenido de filtrado Websense y N2H2, por lo que se mostrara que CBAC realiza la inspeccion de la capa de aplicación y es un requisito para ejecutar filtro de URL.

LOCALIZACION DEL SERVIDOR DE CONTENIDO

Un punto muy importante que se necesita tomar en cuenta en el filtro de contenido web en un router es la localizacion de el Nuevo servidor de filtro de contenido: es decir; ¿dónde deberia colocarse este dispositivo en la red? Una preocupación

principal con el router y el filtro de url es el tiempo de respuesta entre el servidor de filtro de contenido y el router.

En el proceso de filtro de URL, el router reenvia las solicitudes de usuario a un servidor web externo y el envia una petición de acceso al servidor de contenido. Si el servidor web externo contesta de regreso al router antes de que la politica se tome en cuenta en el servidor de filtro de contenido, el router almacena las respuestas en el servidor externo, el cual introduce un retraso en el flujo del tráfico y coloca una carga adicional en el router. Las ultimas respuestas que el router recibe de el servidor de filtro de contenido, siendo mas el impacto que tendra en el procesamiento.

Por lo tanto, la recomendacion en el diseño de la red es colocar el servidor de contenido en la misma subred como una interface de el router. Sin embargo, a mayor número de dispositivos se encuentren en la subred, la competencia entre los dispositivos que se encuentran alli cuando envien tráfico atraves del router en la misma red, sera mayor. Por lo tanto, es necesario asegurar que existe un suficiente ancho de banda entre el router y el servidor de filtrado de contenido para enlazar el tráfico de comunicación. En una situación con el peor de los casos, se podria necesitar una conexión dedicada en el router para el servidor de contenido.

CONFIGURANDO FILTRO DE URLS

A continuación se explican los comandos que se utilizan para configurar al Router para que útilice el servidor de filtrado de contenido.

LOCALIZACION DEL SERVIDOR

Después que se ha habilitado la inspección para el tráfico HTTP, se debe especificar el tipo y localización del servidor de filtrado de contenido. Este es requerido por el router para filtrado de URL. Para especificar esta información se debe usar el siguiente comando:

Router(config)# ip urlfilter server vendor

{websense | n2h2} IP_address [port port-number] [timeout seconds]
[retransmit number]

El comando ***ip urlfilter audit. vendor*** especifica como conectar el servidor de filtrado de contenido. Este primer parámetro que se debe especificar es que producto de servidor de filtro de contenido se utilizara: Websense o N2H2. Después de esto la dirección IP del servidor. Los cuatro parámetros restantes son opciónales. Para un servidor N2H2, el número de puerto por defecto es 4005; Websense usa 15,868. Si se cambia el número de puerto durante la instalación, se necesita reflejar el cambio con el parámetro del puerto.
Seguido de esto el valor del timeout para la conexión del servidor. Esta es la suma del tiempo que el router esperara por una respuesta del servidor de filtrado de contenido; sino se considera ninguna respuesta dentro de este limite de tiempo, el router utiliza un segundo servidor, si este es configurado. El tiempo de vida por defecto es de cinco segundos. El router también retransmite peticiones cuando una respuesta no llega del servidor. El número de retransmisiones por defecto es dos, pero esto puede ser modificado con el parámetro de retransmisión.

Se pueden entrar múltiples servidores, pero el primero que se introduce es el servidor primario. Por lo tanto, el orden en que se introduzca el servidor es importante.

DOMINIOS EXCLUSIVOS

El filtrado de URL pone una carga adicional en el router, especialmente si el router constantemente debe enviar peticiones de las operaciones de búsqueda al servidor de filtrado de contenido. Se puede reducir el número de operaciones de búsqueda de dos maneras:

Creando un tamaño más grande de caché.
Usando dominios exclusivos.

Los dominios exclusivos permiten la definición de reglas de filtrado local en el router. En esta situación, el router primero busca en el caché para ver si existe un enlace, luego busca los dominios localmente enumerados y entonces envía una petición al servidor de filtro de contenido si no encuentra nada localmente en el router. Esta configuración es muy útil para la lista de sitios que siempre o nunca deben ser permitidos (y estos sitios nunca cambian). Comúnmente se utilizan sitios que deberían estar listados. Por ejemplo, si el administrador de red constantemente accede al sito WEB de cisco, se debe incluir una acción de permiso en la configuración de domino exclusivo.

Este es el comando para definir un domino exclusive:

Router (config) # ip urlfilter exclusive-domain
{permit | deny} domain_name

Se pueden especificar dos acciones: permitir o denegar. Cuando se especifica un nombre de dominio, se puede ser muy especifico, como por ejemplo detallando: www.quizware.com. Un nombre de domino parcial, como: .quizware.com o un nombre de dominio completamente calificado y un URL parcial, como www.quizware.com/dealgroup. Se puede listar muchos entradas de nombre de dominios como se quieran.

Con las siguientes sentencias se muestran como definir dos dominios que siempre deberían estar permitidos y uno que siempre debería estar negado:

Configurando Dominios Exclusivos para filtrado de URL

Router (config) # ip urlfilter exclusive-domain permit .cisco.com

Router (config) # ip urlfilter exclusive-domain permit .quizware.com

Router (config) # ip urlfilter exclusive-domain deny .sex.com

LA CONEXION AL SERVIDOR SE DA POR PERDIDA

Algunas veces la IOS Cisco no es capaz de entrar en contacto con el servidor de filtrado de contenido para autorizar a los usuarios la conexión HTTP. Por ejemplo, se podría tener que resetear el servidor a los rendimientos del sistema que se han aplicado. En este caso, la IOS Cisco toma una de dos acciones que tengan que ver con el tráfico HTTP durante este periodo de bloqueo:

Descartar todo el tráfico hasta que la conexión entre el router y el servidor de filtrado de contenido URL se restaura.

Permitir todo el tráfico hasta que la conexión entre el router y el servidor de filtrado de contenido URL se restaura.

Por defecto, todo el tráfico se descarta pero, esto puede ser modificado con el siguiente comando:

Router (config) # ip urlfilter allowmode [on | off]

"On" especifica que la petición de conexión debería permitirse cuando el router no puede alcanzar el servidor de filtrado de contenido. **Off** especifica que la udit. no debería descartarse.

Siempre que el router pierda contacto con el servidor de filtrado de contenido, un mensaje de alerta es mostrado, junto con el estado del modo que el router esta usando. Con la siguiente sentencia, el router descarta el tráfico hasta que la udit. no entre el router y el servidor se re-establece:

%URLF-3-ALLOW_MODE: Connection to all URL filter servers are down and ALLOW MODE if OFF

MÁXIMO DE SOLICITUDES

La IOS Cisco soporta temporalmente hasta 1000 peticiones URL pendientes. Estas son peticiones que la IOS Cisco tiene que enviar al servidor de contenido y esperar por una respuesta de parte de el. Cuando se alcanza el límite, una conexión de un nuevo usuario es descartada, haciendo que el buscador WEB del usuario realice una

retransmisión. Para cambiar el número de solicitudes pendientes que la IOS Cisco almacene, se utiliza el siguiente comando:

Router (config) # ip urlfilter max-request #_of_requests

El número de peticiones que pueden especificarse oscila en un rango de 1 a 2,147,483,647.

MAXIMO DE RESPUESTAS

Un router puede llegar a recibir el tráfico HTTP de regreso del servidor WEB externo antes de que se reciba la respuesta de la política de seguridad del servidor de filtrado de contenido. En este caso, el router puede almacenar las respuestas http mientras se espera por la respuesta del servidor de filtrado. Sin embargo, por defecto, el router almacena solo 200 respuestas de conexión. Esto puede ser cambiado con el siguiente comando:

Router (config) # ip urlfilter max-resp-pak #_of_responses

El número de respuesta de la IOS Cisco puede almacenarse en un rango de 0 a 20,000.

ALERTAS

Las alertas del filtrado de URL están habilitadas por defecto. Estas alertas muestran mensajes donde el servidor de filtrado de contenido no es alcanzable, cuando todos los servidores no son accesibles o cuando las operaciones de búsqueda de URL exceden el valor de tiempo de vida. Las alertas pueden ser deshabilitadas o re-habilitadas con el siguiente comando:

Router (config) # [no] ip urlfilter alert

INTERVENCIONES

Como con las intervenciones de CBAC, la intervención de filtrado de URL están deshabilitadas por defecto. Habilitar las intervenciones permite registrar información como quien realiza solicitudes de conexión HTTP y que servidor WEB esta tratando de acceder. Para habilitar las intervenciones, se utiliza el siguiente comando:

Router (config) # [no] ip urlfilter audit.-trail

INSPECCIÓN DE CBAC

Para instalar la inspección de URLs, se necesita configurar CBAC para la inspección de HTTP. Esto se requiere para realizar filtrado de URL. A continuación se presenta el comando de CBAC:

Router (config) # ip inspect name inspection_name http urlfilter
[java-list ACL_#_or_name]
[alert {on | off}] [audit-trail {on | off}] [timeout seconds]

Es necesario especificar la palabra clave de urlfilter para habilitar el filtro de contenido para conexiones http. Si se omite tal palabra, la inspeccion de http se hace con un filtro de Java.
Es altamente recomendado que se especifique un ACL para limitar el alcance de Java o el filtro de URL. De lo contrario, el router tendría que examinar todas las solicitudes de conexión http, siendo demasiado para CPU.

CONFIGURACIÓN SIMPLE PARA FILTRAR CONTENIDO URL EN EL ROUTER

Router (config) # ip inspect name RULES http urlfilter (1)
Router (config) # ip inspect name RULES ftp
Router (config) # ip inspect name RULES smtp
Router (config) # ip inspect name RULES tcp
Router (config) # ip inspect name RULES udp

Router (config) # ip urlfilter server vendor websense 192.1.2.2 (2)

Router (config) # ip urlfilter cache 7000 (3)

Router (config) # ip urlfilter max-request 1500 (4)

Router (config) # ip urlfilter max-resp-pack 300 (5)

Router (config) # ip urlfilter exclusive-domain permit .cisco.com (6)

Router (config) # ip urlfilter exclusive-domain permit www.quizware.com

Router (config) # ip urlfilter exclusive-domain deny .msn.com

Router (config) # ip urlfilter exclusive-domain deny .aol.com

Router (config) # ip urlfilter audit-trail (7)

Router (config) # ip urlfilter alert

Router (config) # ip urlfilter urlf-server-log

Router (config) # ip access-list extended external_ACL

Router (config-ext-nacl) # ! ←enter ACL policies here→
Router (config-ext-nacl) # deny ip any any
Router (config-ext-nacl) # exit

Router (config) # interface Ethernet1

Router (config-if) # ip inspect RULES out (8)

Router (config-if) # ip access-group external_ACL in

1. La primera regla de la inspección en el grupo de las REGLAS especifica la inspección para las conexiones http de filtrado URL.

2. Esta oracion especifica que el servidor de filtrado de contenido está corriendo Websense. Note que este servidor está conectado directamente al router, proporcionando un estado de latencia bajo para las peticiones y las contestaciones.

3. Esta declaración aumenta el tamaño del cache de URL por defecto de 5000 a 7000. hay que recordar que se debe tener cuidado sobre el aumento de este valor: asegurarse de haber evaluado la RAM del router y el procesamiento antes de aumentar las variables de funcionamiento de filtrado de URL.

4. Esta oracion aumenta el número máximo de peticiones a partir de 1000 a 1500; esto controla el número de las peticiones pendientes que la IOS Cisco mantiene mientras espera las respuestas del servidor Websense.

5. Esta declaración aumenta el número máximo de respuestas de los servidores web de 200 a 300 paquetes.

6. Las siguientes cuatro declaraciones configuran exclusivamente el filtro de dominio: Todo el acceso a todos los sitios web de Cisco y www.quizware.com se permiten y cualquier acceso a los nombres de dominio de MSN y de AOL de Microsoft son negados.

7. Los siguientes tres comandos habilitan la revisión y alarmas y reenvio de mensajes de registro de URL al servidor de Websense.

8. La regla de la inspección (REGLAS) es habilitada en la interface externa.

NBAR

PROTOCOLOS Y APLICACIONES QUE SOPORTA NBAR

Protocolos Soportados TCP/IP		
Protocolo	# Protocolo	Descripción
ICMP	1	Internet Control Message Protocol.
IPINIP	4	IP in IP.
EGP	8	Exterior Gateway Protocol.
IPSEC	50 and 51	Protocolo de Seguridad de Internet.

Tabla A-5.5 Listado de protocolos que soporta TCP / IP

Número de Puertos estáticos que soporta:

Parámetro	Protocolo	# Puerto
SSH	TCP	22
PCANYWHERE	UDP	22
TELNET	TCP	23
SMTP	TCP	25
DNS	TCP/UDP	53
DHCP	UDP	67 and 68
GOPHER	TCP/UDP	70
FINGER	TCP	79
HTTP	TCP	80
KERBEROS	TCP/UDP	88 and 749
POP3	TCP/UDP	110
NNTP	TCP/UDP	119
NTP	TCP/UDP	123
NETBIOS	TCP/UDP	137 and 139
NETBIOS	UDP	137 and 138
IMAP	TCP/UDP	143 and 220
SNMP	TCP/UDP	161 and 162
BGP	TCP/UDP	179
IRC	TCP/UDP	194
LDAP	TCP/UDP	389
SECURE-HTTP	TCP	443
SYSLOG	UDP	514
PRINTER	TCP/UDP	515
RIP	UDP	520
SECURE-NNTP	TCP/UDP	563
SECURE-MAP	TCP/UDP	585 and 993
SECURE-LDAP	TCP/UDP	636
SECURE-FTP	TCP	990
SECURE-TELNET	TCP	992
SECURE-IRC	TCP/UDP	994

SECURE-POP3	TCP/UDP	995
SOCKS	TCP	1080
NOTES	TCP/UDP	1352
SQLSERVER	TCP	1433
RSVP	UDP	1698 and 1699
L2TP	UDP	1701
PPTP	TCP	1723
NFS	TCP/UDP	2049
NOVADIGM	TCP/UDP	3460 to 3465
PCANYWHERE	TCP	5631 and 65301
XWINDOWS	TCP	6000 to 6003
CUSEEME	TCP/UDP	7648 and 7649
CUSEEME	UDP	24,032

Tabla A-5.6 Listado de número de puertos

Aplicaciones Soportadas por NBAR

Aplicación	Protocolo
CITRIX CITRIX APP	TCP/UDP
FTP	TCP
EXCHANGE	TCP
FASTTRACK	TCP/UDP
GNUTELLA	TCP
HTTP	TCP
NAPSTER	TCP
KAZAA2	TCP
NETSHOW	TCP/UDP
RCMD	TCP
REALAUDIO	TCP/UDP
RTP	TCP/UDP
SQLNET	TCP/UDP
STREAMWORK	UDP
SUNRPC	TCP/UDP
TFTP	UDP
VDOLIVE	TCP/UDP

Tabla A-5.7 Aplicaciones soportadas por NBAR

SISTEMAS DE DETECCION DE INTRUSOS (IDS) [18]

¿POR QUÉ UTILIZAR UN IDS?

La detección de intrusiones permite a las organizaciones proteger sus sistemas de las amenazas que aparecen al incrementar la conectividad en red y la dependencia que tenemos hacia los sistemas de información.
Los IDS han ganado aceptación como una pieza fundamental en la infraestructura de seguridad de la organización. Hay varias razones para adquirir y usar un IDS:

PREVENIR PROBLEMAS AL DISUADIR A INDIVIDUOS HOSTILES

Al incrementar la posibilidad de descubrir y castigar a los atacantes, el comportamiento de algunos cambiará de forma que muchos ataques no llegarán a producirse. Esto también puede jugar en nuestra contra, ya que la presencia de un sistema de seguridad sofisticado puede hacer crecer la curiosidad del atacante.

DETECTAR ATAQUES Y OTRAS VIOLACIONES DE LA SEGURIDAD QUE NO SON PREVENIDAS POR OTRAS MEDIDAS DE PROTECCIÓN

Los atacantes, usando técnicas ampliamente conocidas, pueden conseguir accesos no autorizados a muchos sistemas, especialmente a aquellos conectados a redes públicas. Esto a menudo ocurre cuando vulnerabilidades conocidas no son corregidas.
Aunque los vendedores y administradores procuran dar a conocer y corregir estas vulnerabilidades, hay situaciones en las que esto no es posible:
En algunos sistemas heredados, los sistemas operativos no pueden ser parcheados o actualizados.
Incluso en los sistemas en los que podemos aplicar parches, los administradores a veces no tienen el suficiente tiempo y recursos para seguir e instalar las últimas actualizaciones necesarias.

Esto es un problema común, sobre todo en entornos que incluyen un gran número de estaciones de trabajo con sistemas operativos y hardware variado.
Los usuarios y administradores pueden equivocarse al configurar sus sistemas.
Un sistema de detección de intrusos puede ser una excelente herramienta de protección de sistemas.
Un IDS puede detectar cuando un atacante ha intentado penetrar en un sistema explotando un fallo no corregido. De esta forma, podríamos avisar al administrador para que llevara a cabo un backup del sistema inmediatamente, evitando así que se pierda información valiosa.

DETECTAR PREÁMBULOS DE ATAQUES (NORMALMENTE PRUEBAS DE RED Y OTRAS ACTIVIDADES)

Cuando un individuo ataca un sistema, lo hace típicamente en fases predecibles. En la primera fase, el atacante hace pruebas y examina el sistema o red en busca de un punto de entrada óptimo. En sistemas o redes que no disponen de un IDS, el atacante es libre de examinar el sistema con un riesgo mínimo de ser detectado. Esto le facilita la búsqueda de un punto débil en nuestra red.

La misma red con un IDS monitorizando sus operaciones le presenta una mayor dificultad. Aunque el atacante puede examinar la red, el IDS observará estas pruebas, las identificará como sospechosas, podrá activamente bloquear el acceso del atacante al sistema objetivo y avisará al personal de seguridad de lo ocurrido para que tome las acciones pertinentes.

DOCUMENTAR EL RIESGO DE LA ORGANIZACIÓN

Cuando se hace un plan para la gestión de seguridad de la red o se desea redactar la política de seguridad de la organización, es necesario conocer cual es el riesgo de la organización a posibles amenazas, la probabilidad de ser atacada o si incluso ya está siendo atacada.

Un IDS nos puede ayudar a conocer la amenaza existente fuera y dentro de la organización, ayudándonos a tomar decisiones acerca de los recursos de seguridad que deberemos emplear en nuestra red y del grado de cautela que deberemos adoptar al redactar la política de seguridad.

PROVEER INFORMACIÓN ÚTIL SOBRE LAS INTRUSIONES QUE SE ESTÁN PRODUCIENDO

Incluso cuando los IDS no son capaces de bloquear ataques, pueden recoger información relevante sobre éstos. Esta información puede, bajo ciertas circunstancias, ser utilizada como prueba en actuaciones legales. También se puede usar esta información para corregir fallos en la configuración de seguridad de los equipos o en la política de seguridad de la organización.

TIPO DE ANÁLISIS

Hay dos acercamientos al análisis de eventos para la detección de ataques: detección de abusos y detección de anomalías. La detección de abusos es la técnica usada por la mayoría de sistemas comerciales. La detección de anomalías, en la que el análisis busca patrones anormales de actividad. La detección de anomalías es usada de forma limitada por un pequeño número de IDS.

DETECCIÓN DE ABUSOS O FIRMAS

Los detectores de abusos analizan la actividad del sistema buscando eventos que coincidan con un patrón predefinido o firma que describe un ataque conocido.

Ventajas:

Los detectores de firmas son muy efectivos en la detección de ataques sin que generen un número elevado de falsas alarmas.

Pueden rápidamente y de forma precisa diagnosticar el uso de una herramienta o técnica de ataque específico. Esto puede ayudar a los encargados de la seguridad a priorizar medidas correctivas.

Pueden permitir a los administradores de seguridad, sin importar su nivel o su experiencia en este campo, el seguir la pista de los problemas de seguridad de sus sistemas.

Desventajas:

Solo detectan aquellos ataques que conocen, por lo que deben ser constantemente actualizados con firmas de nuevos ataques. Muchos detectores de abusos son diseñados para usar firmas muy ajustadas que les privan de detectar variantes de ataques comunes.

DETECCIÓN DE ANOMALÍAS

La detección de anomalías se centra en identificar comportamientos inusuales en una estación de trabajo o una red.

Funcionan asumiendo que los ataques son diferentes a la actividad normal. Los detectores de anomalías construyen perfiles representando el comportamiento normal de los usuarios, estaciones de trabajo o conexiones de red. Estos perfiles son construidos de datos históricos recogidos durante el periodo normal de operación. Los detectores recogen los datos de los eventos y usan una variedad de medidas para determinar cuando la actividad monitorizada se desvía de la actividad normal. Las medidas y técnicas usadas en la detección de anomalías incluyen:

Detección de un umbral sobre ciertos atributos del comportamiento del usuario. Tales atributos de comportamiento pueden incluir el número de ficheros accedidos por un usuario en un período de tiempo dado, el número de intentos fallidos para entrar en

el sistema, la cantidad de CPU utilizada por un proceso, etc. Este nivel puede ser estático o heurístico.

Medidas estadísticas, que pueden ser paramétricas, donde la distribución de los atributos perfilados se asume que encaja con un determinado patrón, o no paramétricas, donde la distribución de los atributos perfilados es aprendida de un conjunto de valores históricos, observados a lo largo del tiempo.
Otras técnicas incluyen redes neuronales, algoritmos genéticos y modelos de sistema inmune.

Solo las dos primeras se utilizan en los IDSs actuales, el resto son parte de proyectos de investigación.

Ventajas:
Los IDSs basados en detección de anomalías detectan comportamientos inusuales. De esta forma tienen la capacidad de detectar ataques para los cuales no tienen un conocimiento específico.

Los detectores de anomalías pueden producir información que puede ser utilizada para definir firmas en la detección de abusos.

Desventajas:
La detección de anomalías produce un gran número de falsas alarmas debido a los comportamientos no predecibles de usuarios y redes.

Requieren conjuntos de entrenamiento muy grandes para caracterizar los patrones de comportamiento normal.

FUNCIONAMIENTO DE LOS IDS

Los IDS son parte de las defensas que deben utilizarse en los sistemas de transmisión de datos, ya que son capaces de alertarnos acerca de toda actividad sospechosa que típicamente ocurre antes y durante un ataque.

Un IDS es aquel que tiene como función el detectar y alertar sobre las intrusiones intentadas en un sistema o en la red. Se considera que una intrusión es toda actividad no autorizada o no deseada ocurrida en ese sistema o red.

Los IDS básicamente son una máquina de decisión, capturar un determinado dato y deciden si es un ataque o no en función de una colección de datos etiquetados relevantes almacenados en una base de datos. El inconveniente es que los IDS "clásicos" hacen esta decisión de una manera muy mecánica. Comparan el dato (paquete) recibido contra todos los demás que posee en su base de datos y si se da una coincidencia exacta, se decide si es un ataque o no.

Para realizar su labor, muchos IDS's basan sus operaciones en el análisis de un seguimiento realizado sobre el sistema operativo. Los datos asi obtenidos constituyen una "huella" del uso del sistema a lo largo del tiempo. A partir de esta información, los IDS's calculan métricas sobre el estago global del sistema y deciden si en un momento determinado el sistema esta sufriendo algún tipo de intrusión. Los IDS's también pueden realizar su propio sistema de monitoreo, manteniendo un conjunto de estadísticas que ofrecen un perfil del uso del sistema. Las estadísticas citadas pueden ser obtenidas de varias fuentes como pueden ser:

El uso de la CPU, las entradas y salidas del disco, el uso de memoria, las actividades realizadas por los usuarios, el número de conexiones intentadas, etc. Estos datos deben ser actualizados continuamente para reflejar el estado actual del sistema y a partir de un modelo interno, el IDS determinara si una serie de acciones constituyen una intrusión o un intento de intrusión.

El modelo interno mencionado puede describir un conjunto de escenarios de intrusión o posibles perfiles de un sistema sin intrusiones. El IDS es un aparato lo suficientemente pesado como para tener en cuenta lo siguiente:

Nunca debe colocarse de forma que interfiera el funcionamiento de la red, cuanto mas invisible y transparente sea es mejor.
Debe tener suficiente capacidad de procesamiento para procesar todo el tráfico en tiempo real. Si no es suficiente, se debe instalar un equipo mas potente o se debe simplificar el análisis, pero jamás se debe permitir la perdida de paquetes.
No se debe apurar la capacidad de la máquina. Aunque en una situación estacionaria la máquina puede funcionar bastante bien, hay que tener en cuenta que un ataque puede camuflarse en una tormenta de tráfico, destinada a confundir al administrador con cantidades de logs y a sobrecargar los IDS presentes. En una situación normal, la carga de CPU nunca deberia superar el 25%.

DIFERENCIA ENTRE UN IDS Y UN FIREWALL

Un firewall esta diseñado para bloquear o dejar pasar el tráfico en la red por los puertos especificados, es decir cierra las puertas por el cuál se puedan introducir a nuestro sistema, solo dejando abiertos aquellos puertos que el administrador de red desee utilizar. Este fin es para reducir las entradas a nuestro sistema, evitando tener abierto puertos que no esten siendo utilizados.

En cambio el IDS esta destinado para inspeccionar el tráfico en la red, es una alarma que puede indicar en tiempo real si se esta realizando una intrusión, si se sospecha de una o si ya se realizo. Podriamos comparar al Firewall como las cerraduras y protecciones de una casa (bloquean entradas) y al IDS como al vigilante de ella.

Los sistemas de detección de intrusos son una combinación de los sistemas que alertan anticipadamente y los que alarman que algo ha ocurrido y esto es muy diferente a lo que realizan los Firewall.

ALCANCES Y LIMITACIONES DE UN IDS

Se realizan las dos grandes distinciones siguientes:

POSIBILIDADES DE UN IDS

- Aumentar el nivel de seguridad general de nuestro entorno.
- Vigilar el tráfico de red dentro de los mensajes de red.
- Examinar los contenidos de los mensajes de red.
- Detectar los cambios en archivos y directorios.
- Detectar tiempos de acceso normales.
- Alertar ante patrones de ataque conocidos, disminuyendo el número de intrusiones comunes que pueden impactar en la red.
- Detectar errores de configuración en los equipos, descubriendo tráfico procedente de máquinas ajenas a nuestra red.

LIMITACIONES DE LOS IDS

- Eliminar por completo los problemas de seguridad.
- Reemplazar al personal calificado en seguridad en redes o la ayuda externa especializada.
- No reacciona adecuadamente ante nuevos ataques o modificaciones pequeñas hechas a otros paquetes, en donde la vulnerabilidad explotada es totalmente nueva (Aplica principalmente para los IDS clásicos).
- No puede detectar ataques en una comunicación cifrada extremo-extremo (por ejemplo, con SSH), ya que la carga del paquete (payload) va cifrado y no es reconocible.
- No compensa la presencia de mecanismos de autenticación débiles. Si un usuario usa una contraseña sin cifrar (por ejemplo: Telnet, FTP, http, etc.) y alguien la intercepta, el atacante parecera ser un usuario válido y podra hacer todo lo que puede hacer el usuario autentico, sin que el IDS lo detecte.

- No puede automatizar la investigación de los incidentes. Es necesaria la intervención humana (de un analista cualificado) para descubrir la naturaleza real de un ataque, limpiar sus efectos, descubrir al atacante y protegerse para el futuro.
- No compensa la presencia de implementaciones débiles de la pila de protocolos. Este tipo de implementaciones (tanto más débil, cuanto mas se aleje del estándar) producen multitud de falsos positivos, que pueden ayudar a disfrazar un ataque real.
- No es capaz de manejar por si solo todas las configuraciones de red/dispositivos que existen, sobre todo en entornos atípicos (por ejemplo: maquinaria medica conectada a la red, etc). Este tipo de configuraciones utilizan implementaciones propietarias de protocolos que pueden confundir a un IDS, provocando muchos falsos positivos.

REACCIONES DEL IDS: PASIVOS VERSUS REACTIVOS

Otra forma de categorizar los sistemas de detección de intrusos es según su naturaleza de la respuesta:
Pasiva
Reactiva

Los sistemas pasivos simplemente detectan la potencial violacion de seguridad, registran la información y generan un alerta.

Los sistemas reactivos, por el otro lado, estan diseñados para responder ante una actividad ilegal, por ejemplo, sacando al usuario del sistema o mediante la reprogramacion del Firewall para impedir tráfico de red desde una fuente presumiblemente hostil.

DIFERENTES CLASIFICACIONES DE LOS IDS

Los sistemas de detección de intrusos se pueden clasificar, en un primer nivel en dos grandes categorías, de estas se deriva una tercera, estas son las siguientes:

NIDS (Network Intrusion Detection System): Sistemas que analizan el tráfico de la Red Completa.
HIDS (Host Intrusion Detection System): Sistemas que analizan el tráfico sobre un Servidor o PC.
IDS Híbridos. Es la combinación de las ventajas de los dos IDS anteriores.
Cada uno de estos posee las siguientes características:

IDS basados en hosts: Este tipo de IDS's monitorizan log's de eventos de actividades sospechosas procedentes de diversas fuentes. Estas herramientas son especialmente útiles para detectar intrusiones iniciadas por usuarios habituales en el sistema o usuarios que se filtran atraves de la red. Los fallos son detectados muy rapidamente lo que hace a estas herramientas de deteccion muy populares. Abacus Project, Kane Secure Enterprise KSE, RealSecure OS Sensor o Intruder Alert son ejemplos de productos de este tipo.

IDS basado en red (NIDS): Básicamente es un Sniffer, monitoriza el tráfico de la red y además detecta tráfico no deseable. Algunos productos de este tipo son Snort, Defense Worx IDS, Network Flight Recorder, RealSecure, SHADOW.

IDS híbrido: Consiste en la combinación de los dos anteriores proporcionando una máxima seguridad en la red, sin embargo esto supone un gasto importante, por lo que se suele reservar para servidores críticos. En el futuro se estima que serán los más utilizados. Pertenecen a este tipo productos como: CentraxICE, CyberCop Monitor y RealSecure Server Sensor.

Actualmente existen sobre 88 productos IDS distintos, por lo tanto, a continuación se introduciran funciones y características generales de los dos tipos de IDS's más populares: los basados en host y los basados en red.

¿DÓNDE COLOCAR UN IDS?

La decisión de donde localizar el IDS es la primera decisión que hay que tomar una vez que se desea hacer uso de un IDS. De esta decisión dependerá tanto el equipo que usemos, como el software IDS o la base de datos.

Organización

Existen principalmente tres zonas en las que podríamos poner un sensor, tal y como se muestra en la figura:

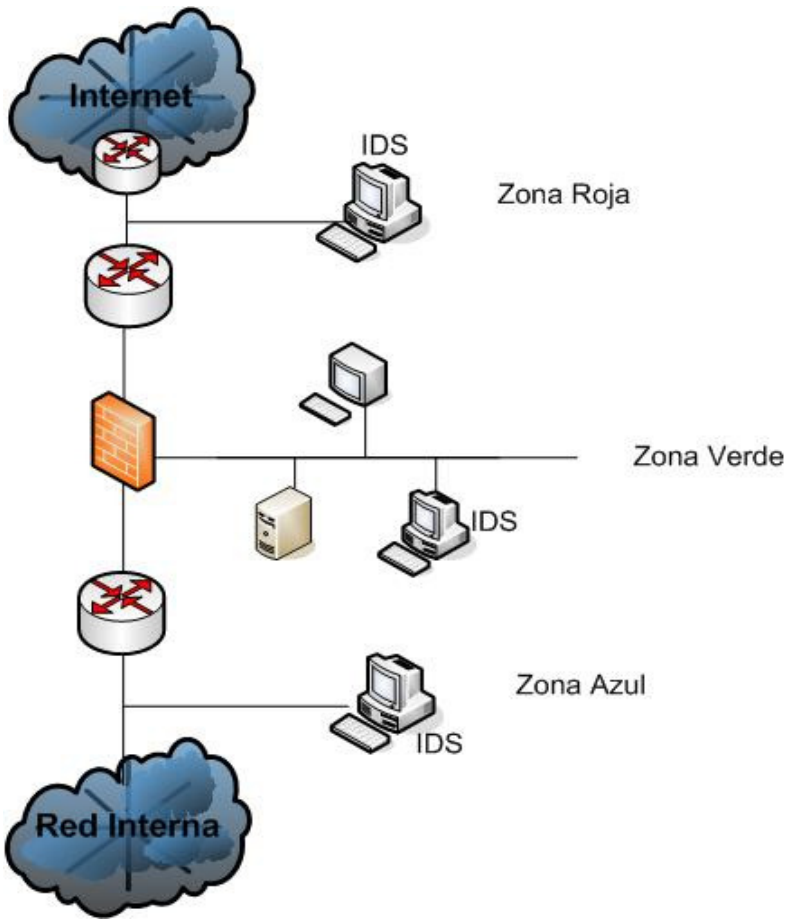


Figura A-5.1 Zonas en las cuales podemos usar IDS

Veamos las características que presenta cada una de estas zonas:

Zona roja: Esta es una zona de alto riesgo. En esta zona el IDS debe ser configurado para ser poco sensible, puesto que vera todo el tráfico que entre o salga de nuestra red y habrá más posibilidad de falsas alarmas.

Zona verde: El IDS debería ser configurado para tener una sensibilidad un poco mayor que en la zona roja, puesto que ahora, el Firewall deberá ser capaz de filtrar algunos accesos definidos mediante la política de nuestra organización. En esta zona aparece un menor número de falsas alarmas que en la zona roja, puesto que en este punto solo deberían estar permitidos accesos hacia nuestros servidores.

Zona azul: Esta es la zona de confianza. Cualquier tráfico anómalo que llegue hasta aquí debe ser considerado como hostil. En este punto de la red se producirán el menor número de falsas alarmas, por lo que cualquier alarma del IDS debe de ser inmediatamente estudiada.

Es importante destacar que la zona azul no es parte de la red interna. Todo lo que llegue al IDS de la zona azul ira hacia el Firewall (por ejemplo, si utilizamos un proxy-caché para nuestros usuarios de WEB) o hacia el exterior. El IDS no escuchará ningún tipo de tráfico interno dentro de nuestra red.

En el caso de tener un IDS escuchando tráfico interno (por ejemplo, colocado entre una VLAN y su router), las falsas alarmas vendrán provocadas en su mayor parte por máquinas internas al acceder a los servidores de nuestra red, por servidores nuestros (DNS sobre todo) y escaneadores de red, por lo que habrá que configurar el IDS para que no sea muy sensible.

NAT [3]

NAT ESTÁTICO

Usamos NAT estático cuando las direcciones están almacenadas en una tabla de consulta del router y se establece un mapeo directo entre las direcciones internas locales y las direcciones internas globales. Eso significa que por cada dirección interna local existe una dirección interna global. Este mecanismo se suele usar cuando se quiere cambiar un esquema de direcciones de una red a otro esquema de direcciones o cuando se tienen servidores que tienen que mantener una dirección IP fija de cara al exterior como DNS o servidores Web.

CONFIGURACIÓN DE NAT ESTÁTICO

Para configurar NAT estático seguiremos los siguientes pasos:
Definir el mapeo de las direcciones estáticas:
"ip nat inside source static local-ip global-ip"
"ip nat inside source static network local-network global-network mask"
Especificar la interfaz interna
"ip nat inside"
Especificar la interfaz externa
"ip nat outside"

NAT DINÁMICO

Usamos NAT dinámico cuando disponemos de un conjunto de direcciones globales internas que se asignarán de forma dinámica y temporal a las direcciones locales internas. Esta asignación se efectuará cuando se recibe tráfico en el router y tiene un Temporizador asignado.

CONFIGURACIÓN DE NAT DINÁMICO

Para configurar NAT dinámico seguiremos los siguientes pasos:
Crear un conjunto de direcciones globales:
"ip nat pool name start-ip end-ip {netmask mask | prefix-length prefix-length}"

Crear una ACL que identifique a los hosts para el traslado:
"access-list access-list-number permit source {source-wildcard}"

Configurar NAT dinámico basado en la dirección origen:
"ip nat inside source list access-list-number pool name"

Especificar la interfaz interna
"ip nat inside"

Especificar la interfaz externa
"ip nat outside"

NAT OVERLOAD O PAT (PORT ADDRESS TRANSLATION)

Usamos PAT (NAT por puertos) cuando disponemos de una dirección global interna que puede direccionar todo un conjunto grande (centenares) de direcciones locales internas. Esta asignación la efectúa cuando el par dirección global/puerto. Aunque disponemos de 65535 puertos (16 bits) en realidad el router PAT solo puede usar un subconjunto de estos puertos (depende del router, pero aproximadamente unas 4000 puertos por dirección global). PAT se puede usar en conjunción con NAT dinámico de forma que varias direcciones globales con múltiples puertos se trasladen a un mayor número de direcciones locales internas.

CONFIGURACIÓN DE PAT

Para configurar PAT seguiremos los siguientes pasos:

Crear un conjunto de direcciones globales (puede ser una sola dirección):
"ip nat pool name start-ip end-ip {netmask mask | prefix-length prefix-length}"

Crear una ACL que identifique a los hosts para el traslado
"access-list access-list-number permit source {source-wildcard}"

Configurar PAT basado en la dirección origen
"ip nat inside source list access-list-number pool name overload"

Especificar la interfaz interna
"ip nat inside"

Especificar la interfaz externa
"ip nat outside"

TECNICAS DE ENCRIPTADO
REDES VIRTUALES PRIVADAS (VPN) [7]

INTRODUCCION

Las redes privadas basadas en internet reciben el calificativo de virtuales dado que para una organización o compañía la red muestra como una red privada dedicada y con un uso exclusivo de toda la infraestructura intermedia, aunque realmente todo esto se aleje de la realidad. El tráfico de una red VPN y el tráfico propio de internet atraviesan la infraestructura de esta en una base paquete a paquete.

Sin embargo, toda esta operación es llevada a cabo de manera que el tráfico apropiado alcance los destinos correctos. Dado que todos los usuarios perciben únicamente su propio tráfico, la red da la apariencia de ser suya y solo suya: una red privada virtual.

Técnicamente, cualquier red privada puede ser considerada como virtual dado que emplea una red telefónica conmutada de carácter público para comunicaciones. No obstante, y dado que el punto de vista esta basado en la semántica y no en las características o requisitos de la red. Los conceptos de red privada basada en red telefónica conmutada y red privada virtual basada en internet son diferentes. Los únicos requisitos para redes privadas virtuales basadas en internet se presentan en cuatro areas claves: compatibilidad, interoperabilidad, disponibilidad y evidentemente seguridad.

Compatibilidad

Para que una red privada virtual pueda utilizar Internet, debe ser compatible con el protocolo de Internet IP y la capa 3 del modelo OSI. Resulta obvia esta consideracion con el fin de poder asignar y, posteriormente, utilizar conjuntos de direcciones IP. Sin embargo, la mayoría de redes privadas emplean direcciones IP privadas o no-oficiales, provocando que únicamente unas pocas puedan ser empleadas en la interaccion con Internet. La razon por la que sucede esto es simple: la obtención de un bloque de direcciones IP oficiales suficientemente grande como para facilitar un subneteo resulta imposible. Las subredes simplifican la administración de direcciones, así como la gestión de los enrutadores y conmutadores pero malgastan direcciones muy preciadas.

Actualmente existen tres técnicas básicas con las que se pueden obtener la compatibilidad deseada entre las redes privadas e Internet:

LA CONVERSIÓN A DIRECCIONES INTERNET

La instalación de gateways IP: En estas técnicas, las direcciones Internet oficiales coexistiran con las redes IP privadas en el interior de la información de la

infraestructura de enrutadores y conmutadores de las organizaciones. De este modo, un usuario con una direcciones IP privada puede acceder al exterior por medio de un servidor de direcciones IP oficiales mediante la infraestructura local y sin necesidad de emplear ningún tipo de acción especial.
Por otro lado, las pasarelas o gateways IP trabajan traduciendo de otro protocolo a IP y viceversa. Normalmente, el gateway IP soporta los clientes asignados a un servidor dotado de un sistema operativo de red (NOS) con un cierto protocolo
nativo. El gateway convierte el tráfico desde el protocolo nativo a IP y viceversa (por ejemplo clientes Novell Netware con protocolo IPX).

Por último, **El empleo de técnicas de tunneling**: El tunneling es llevado a cabo entre ambos extremos de la conexión. La fuente encapsula los paquetes pertencientes a otro protocolo en datagramas IP con el fin de poder atravesar la infraestructura de Internet. El proceso de encapsulamiento esta basado en la añadidura de una cabecera IP al datagrama original, el cuál representara la carga o payload. En el extremo remoto, el receptor desencapsulara el datagrama IP (eliminando la cabecera IP), entregando el datagrama original intacto.
Dado que la realizacion del tunneling es relativamente simple, a menudo resulta la manera mas sencilla y económica de llevar a cabo redes privadas virtuales bajo Internet.

SEGURIDAD

La seguridad es a menudo, el primer objetivo perseguido por las organizaciones dado que Internet es considerada una red “demasiado publica” para realizar comunicaciones privadas. Sin embargo y aplicando las correspondientes medidas de proteccion y seguridad, Internet puede convertirse en una red altamente privada y segura.
Para poder alcanzar este punto, toda red privada virtual debe cumplir principalmente tres objetivos de seguridad:

Proporcionar la seguridad adecuada: Un sistema, mínimo de seguridad debe, al menos, validar a los usuarios mediante contraseñas con el fin de proteger los

recursos de accesos no autorizados. Además, la inclusión de métodos de encriptación permitirá la protección del tráfico a lo largo de su tránsito.
Proporcionar facilidad de administración: La elección de seguridad para la VPN debe ser sencilla de administrar, asi como las funciones de administracion deben ser seguras frente a posibles accesos ilegales.

Transparencia hacia los usuarios: El sistema de seguridad en el acceso a la red privada virtual debe ser totalmente transparente a los usuarios.

DISPONIBILIDAD

La disponibilidad viene motivada principalmente por dos variables:
Una accesibilidad plena e independiente del momento y del lugar.
Un rendimiento óptimo que garantice la calidad de servicio ofrecida al usuario final.

La calidad de servicio (QoS – Qualitity of Service) hace referencia a la capacidad que dispone una red par asegurar un cierto nivel de funcionamiento extremo a extremo. La QoS puede venir dada como una cierta cantidad de ancho de banda o como un ancho de banda que no debe sobrepasarse o bien como una combinación de ambas.

Actualmente, la entrega de datos en Internet es realizada de acuerdo a una base de mejor esfuerzo, la cuál no garantiza completamente esta calidad de servicio demandado. No obstante y en un breve espacio de pocos años, Internet sera capaz de suplir esta carencia ofreciendo un soporte para la QoS a través de un conjunto de protocolos emergentes entre los que cabe destacar RSVP (Resource ReSerVation Protocol) y RTP (Real Time Protocol). Hasta ese momento, los proveedores deberan seguir proporcionando la QoS de las VPNs haciendo uso del tráfico CIR de Frame Relay u otras técnicas.

INTEROPERABILIDAD

Las implementaciones de los tres primeros requisitos han provocado la aparición de un cuarto: La interoperabilidad. Los estándares sobre tunneling, autenticación, encripción y modo de operación son de reciente aparición o bien se encuentra en proceso de desarrollo. Por esta razón, previamente a la adquisión de una tecnología VPN se debe prestar una cuidadosa atención a la interoperabilidad extremo-a-extremo. Esta responsabilidad peude residir tanto en el usuario final como en el proveedor de red, dependiendo de la implementación deseada. Una manera de asegurar una correcta interoperabilidad radica en la elección de una solución completa ofrecida por un mismo fabricante. En el caso de que dicho fabricante no sea capaz de satisfacer todos los requisitos, se deberan limitar los aspectos interoperacionales a un subconjunto que englobe aquellos que sean esenciales, además de utilizar únicamente aquel equipamiento que haya sido probado en laboratorios o bien sometido a campos de pruebas. En cualquiera de los casos, se deberan seleccionar fabricantes que se acoplen totalmente a los estándares VPN y adquirir únicamente aquel equipamiento que pueda ser utilizado tanto mediante programa, firmware o modulos plug-in, con el fin de que puedan adecuarse a futuros estándares.

PROTOCOLOS

Una vez vista la relevancia que presentan estas cuatro áreas en el desarrollo de una VPN, se presenta a continuación una breve descripción y una comparativa funcional entre las principales herramientas protocolarias que permiten alcanzar en general unos niveles bastante satisfactorios, principalmente en las áreas de seguridad y compatibilidad.

Después de haber enmarcado las redes virtuales en la teoría es necesario ver paralelamente los protocolos que hacen posible la operación de las redes virtuales que permiten alcanzar en general los objetivos de una manera satisfactoria, principalmente en las areas de mas interés para este documento que es la seguridad, sin dejar atrás el punto principal de una red: La compatibilidad.

ANEXO 6. MANUAL DE USUARIO

Para iniciar con el uso del programa de configuración del router, se abre el explorador web digitando en la dirección: localhost/router_config/ inmediatamente aparece una ventana de inicio en la que debe especificarse usuario y contraseña, para el caso en usuario se digita: **admin** y en contraseña: **admin.**

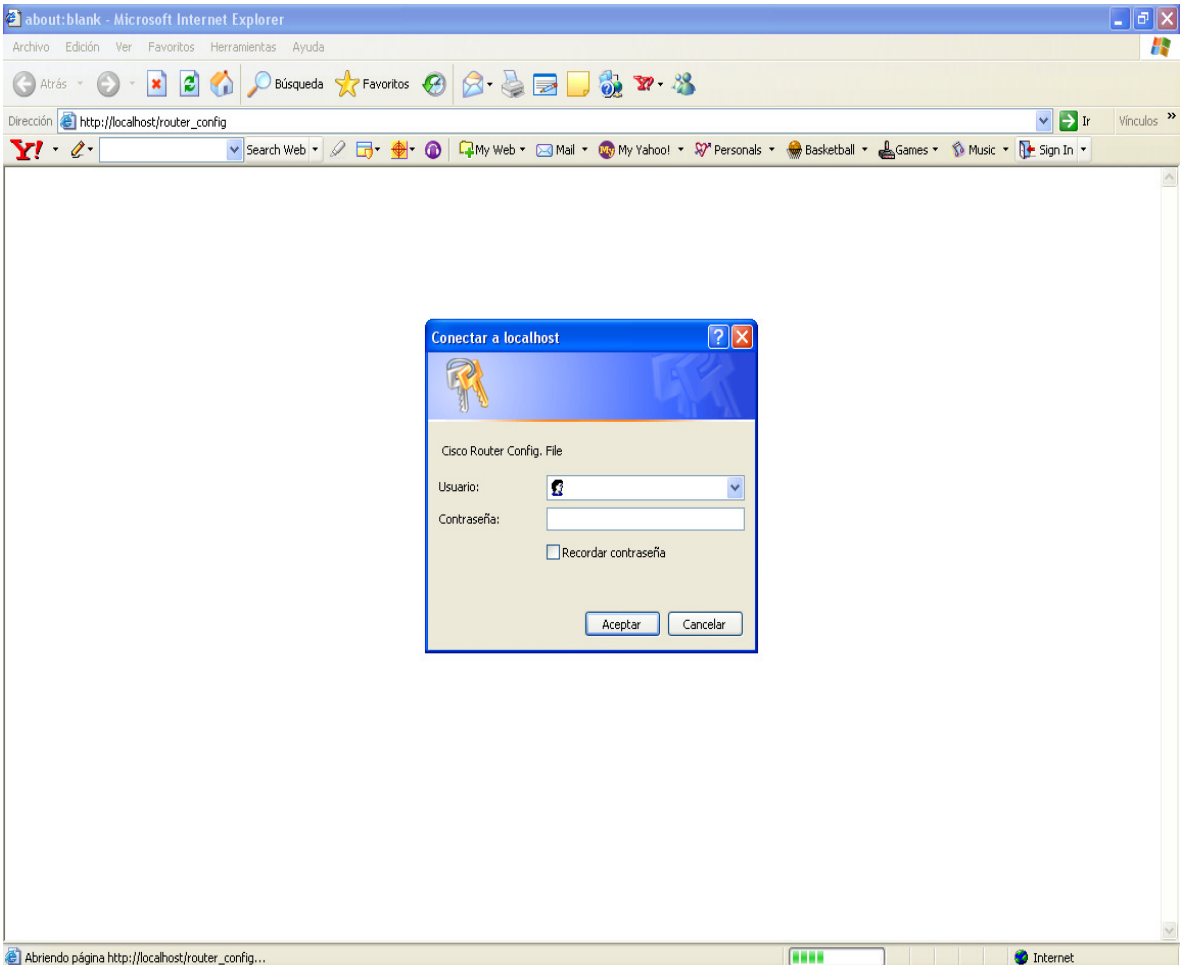


Figura A-6.1 Pantalla de inicio de configuración de router

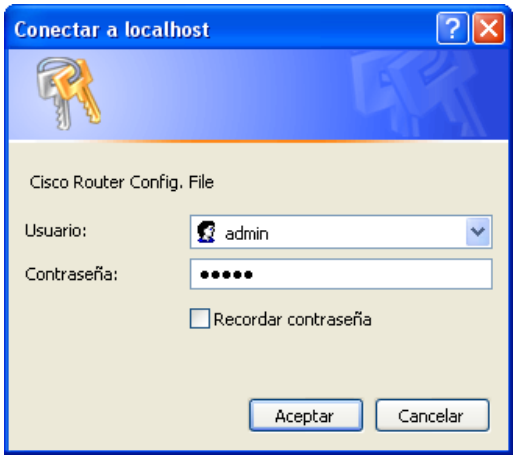


Figura A-6.2 Pantalla con opción de inicio de sesión al sofware de configuración de router

Al ingresar correctamente permite ingresar a la pagina Web que permite la configuración del router, y se debe posicionar sobre el botón Entrar y presionarlo.

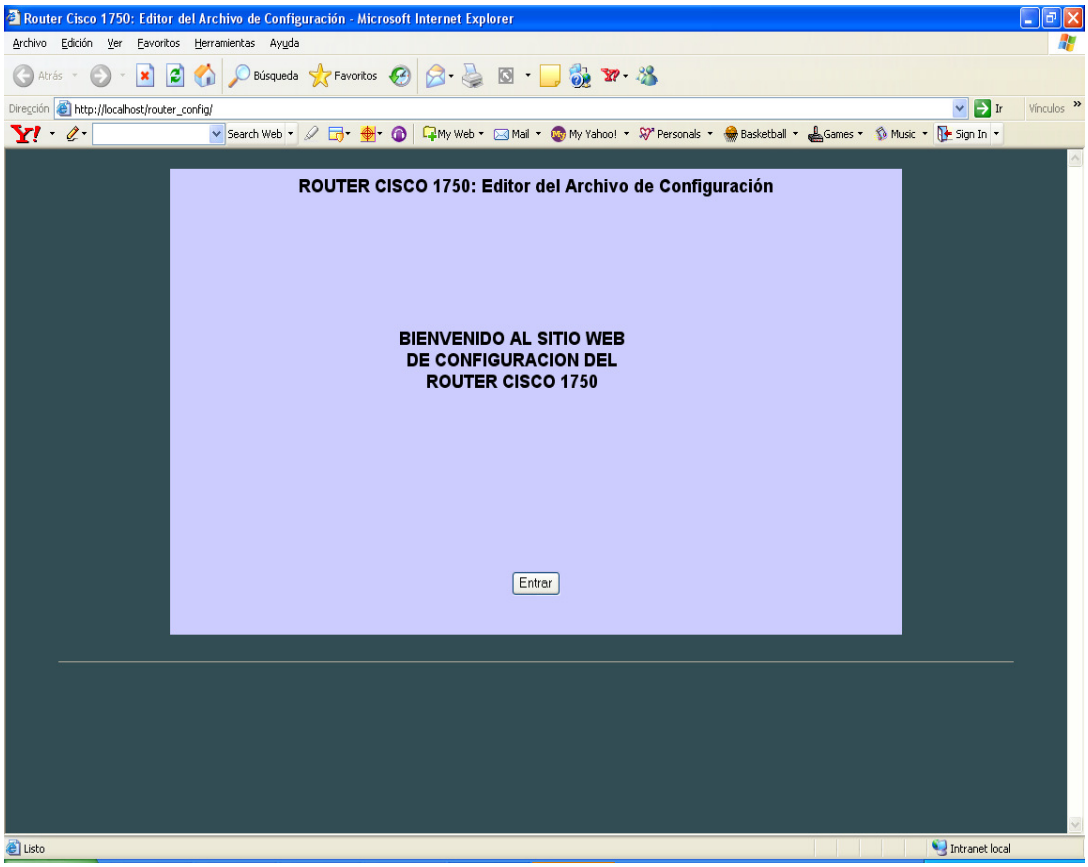


Figura A-6.3 Pantalla de bienvenida al software de configuración de router.

A continuación, se muestra la pantalla de configuración del router, dividiéndose en tres partes, en el que las opciones se muestran en el lado derecho del monitor.

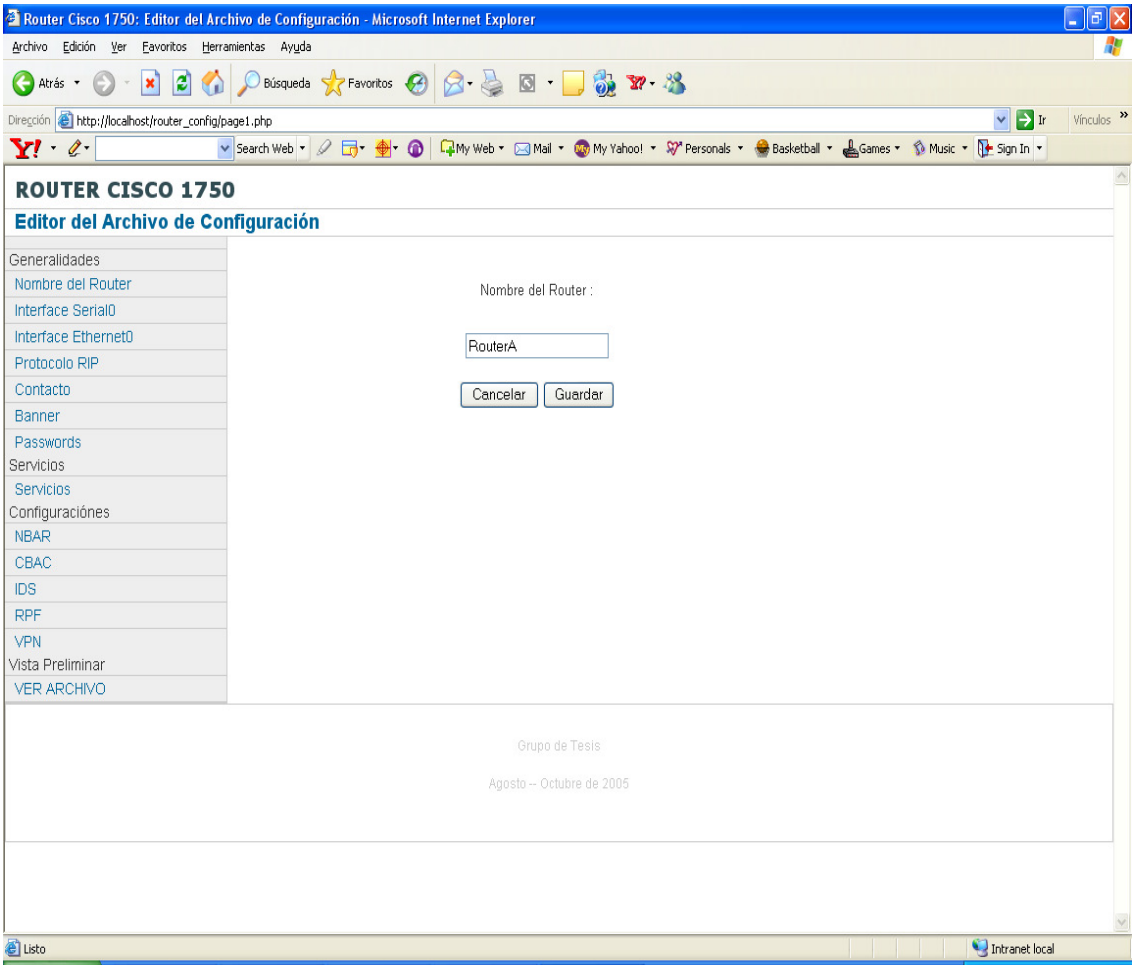


Figura A-6.4 Pantalla inicial de configuración.

La primera página Web configuramos de las Generalidades: en la que se puede definir como primer punto Nombre del Router, luego de haber ingresado el nombre se debe posicionar sobre el el botón Guardar y presionamos, es de mencionar que al pasar el mouse sobre las diferentes opciones de configuración se despliega una ayuda emergente con una breve explicación de la opción que se esta utilizando.

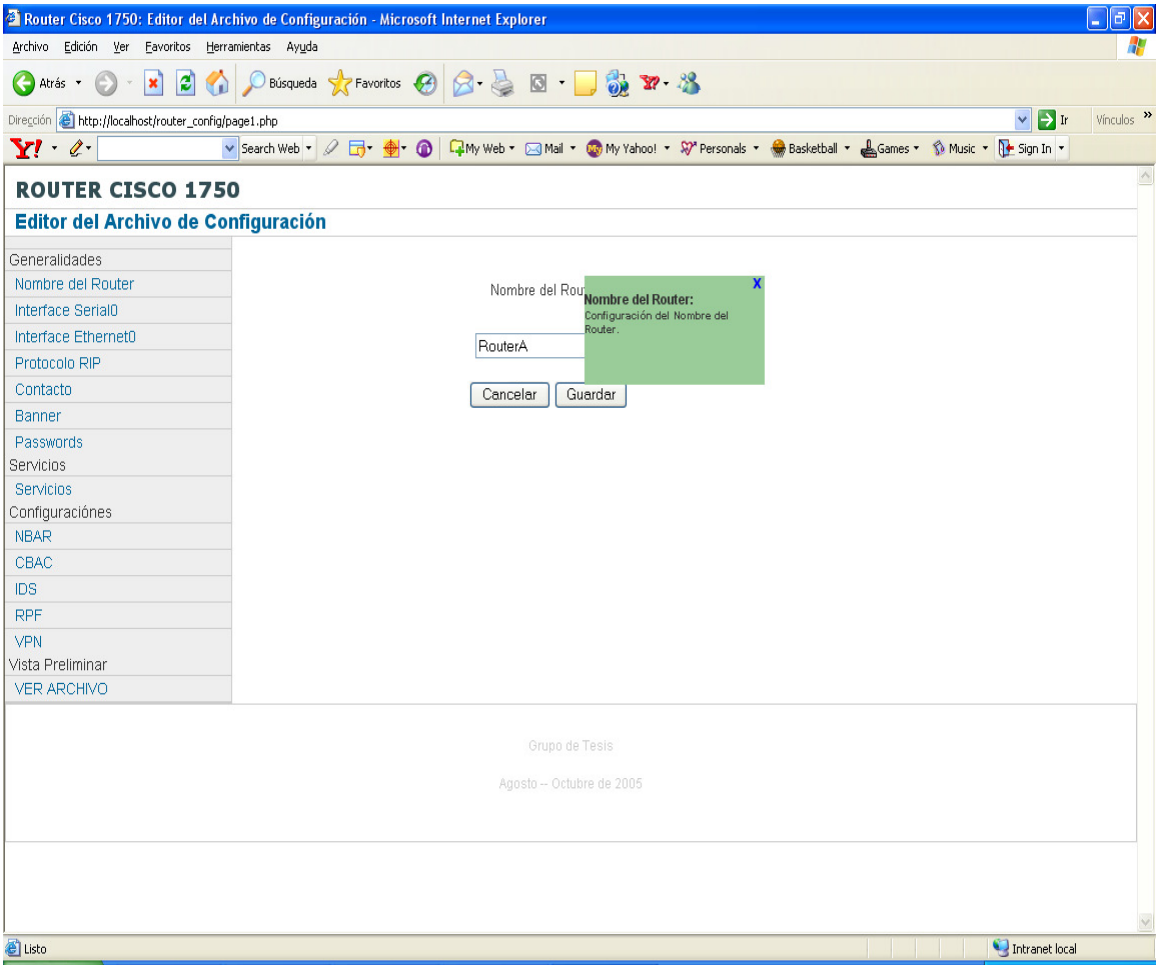


Figura A-6.5 Pantalla donde se especifica el nombre del Router.

El segundo parámetro dentro de las Generalidades es la configuración de la interfaz serial, la que permite ingresar la dirección ip asignada, asi como también la máscare de subred.

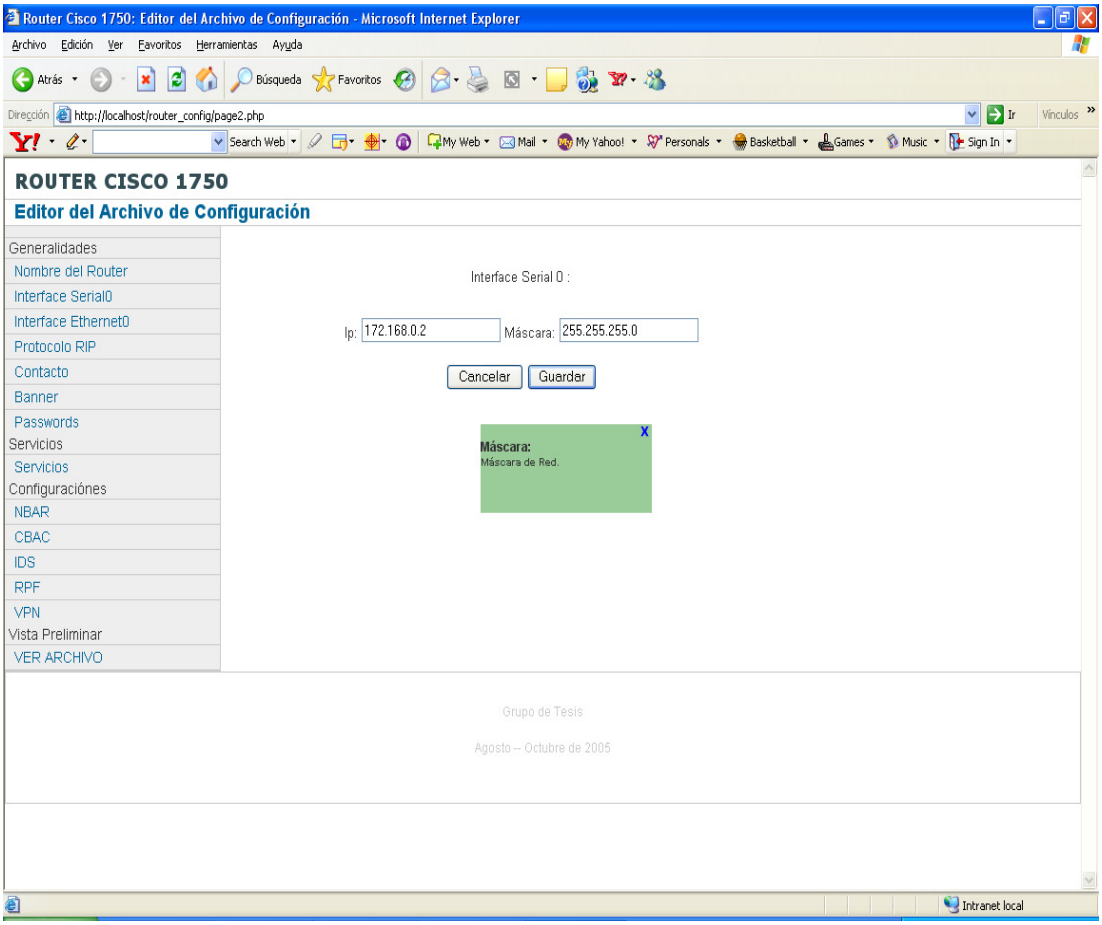


Figura A-6.6 Pantalla donde se definen los valores para interface serial 0.

La siguiente interfaz a configurar es la ehternet, en la cuál ingresamos la ip asignada y la máscara de subred respectiva.

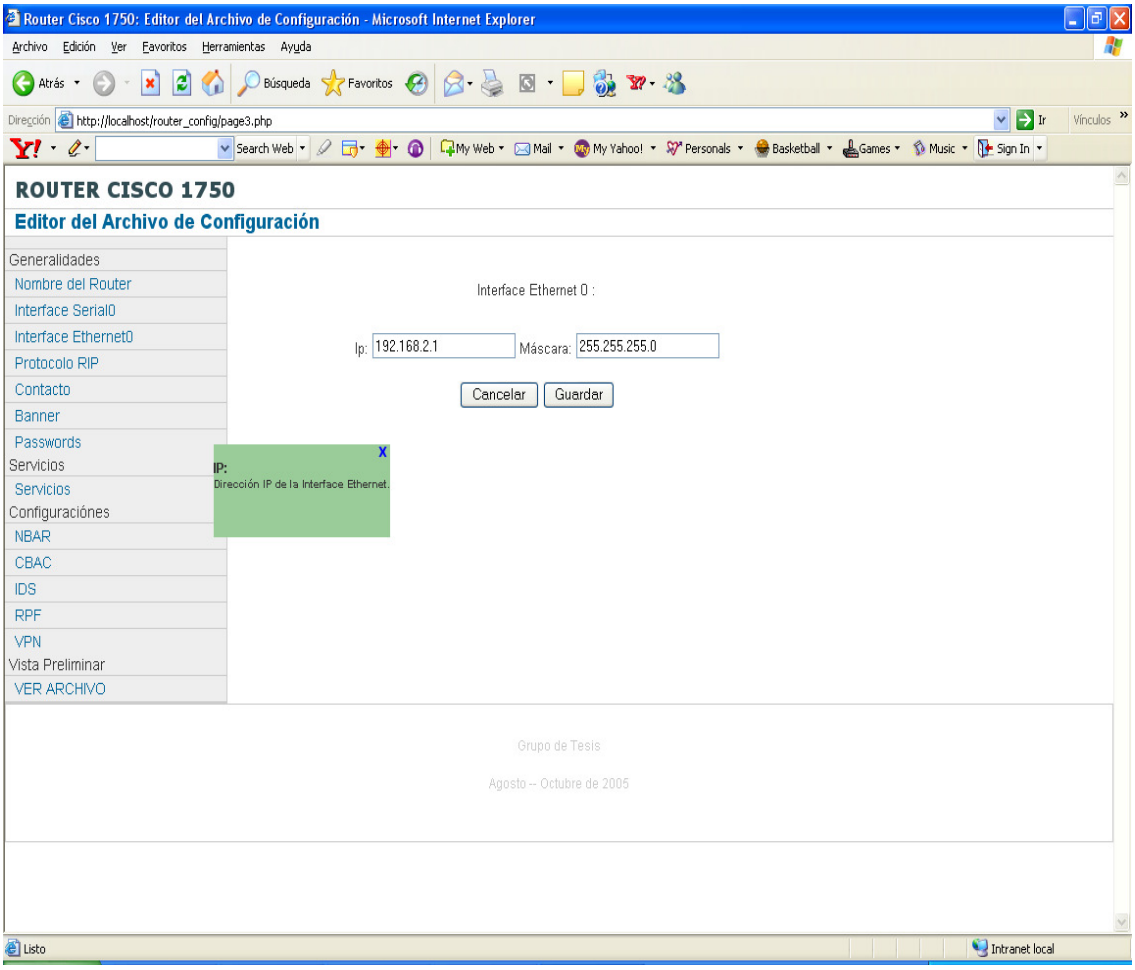


Figura A-6.7 Pantalla donde se puntualizan los valores a definir para la interface ethernet 0.

Luego de realizar la configuración de las interfaces serial y ethernet asignadas procedemos a configurar el protocolo RIP.

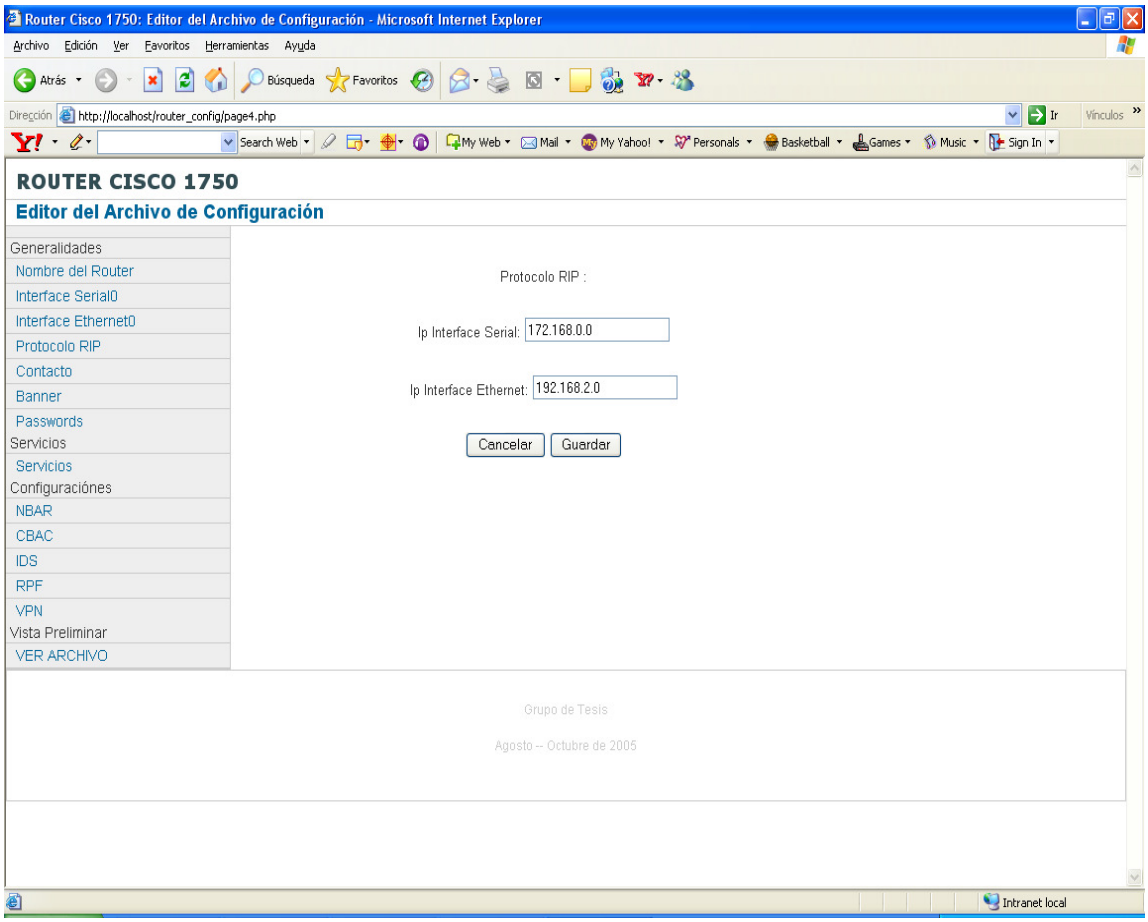


Figura A-6.8 Pantalla donde se definen los valores para protocolo RIP

Luego se introduce como información extra dentro de las generalidades el nombre del contacto (generalmente la persona que configura el router y a quién debería contactarse para cualquier situación, se puede agregar correo electrónico y número telefónico)

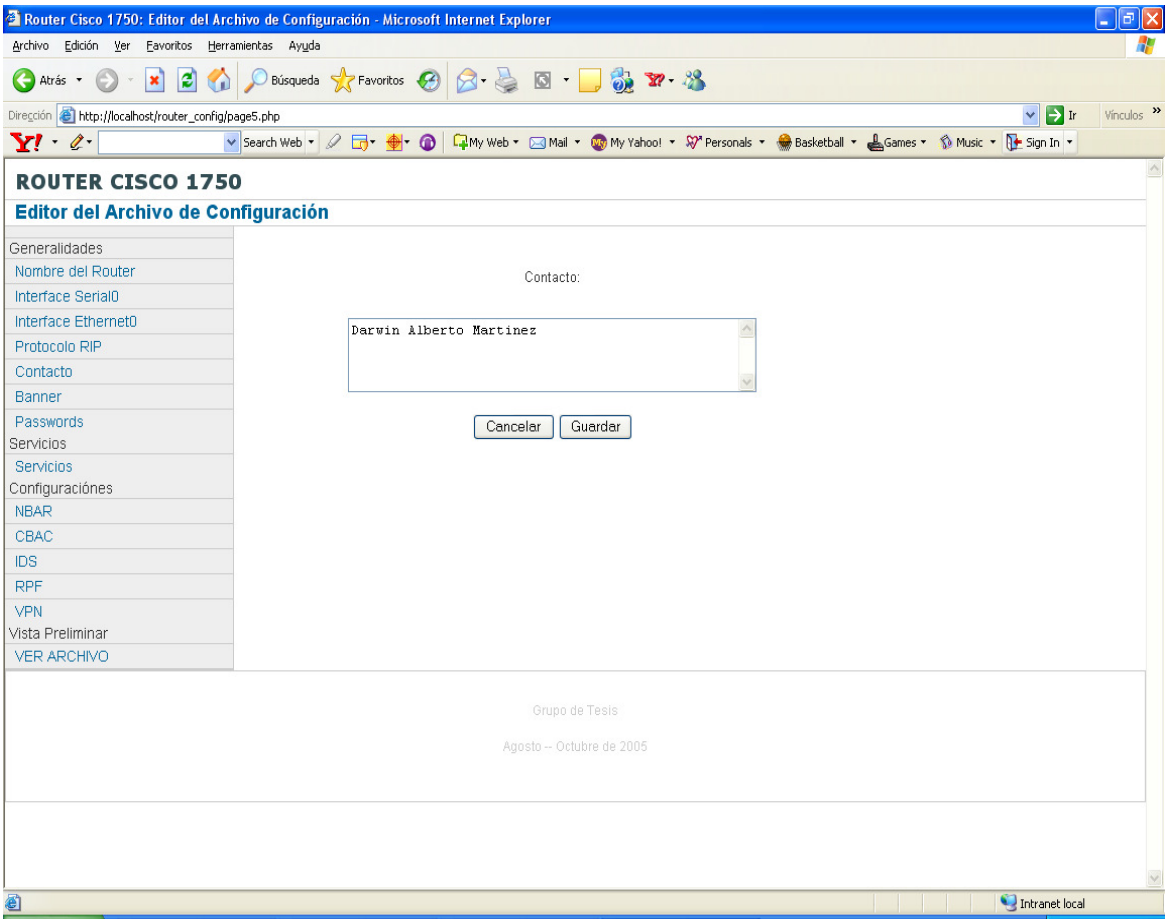


Figura A-6.9 Pantalla donde se especifican datos de la persona que ha realizado las configuraciones del router.

Para concluir la parte de configuración de las generalidades se introduce un mensaje de bienvenida el cuál aparecerá cuando se inicie la configuración del router.

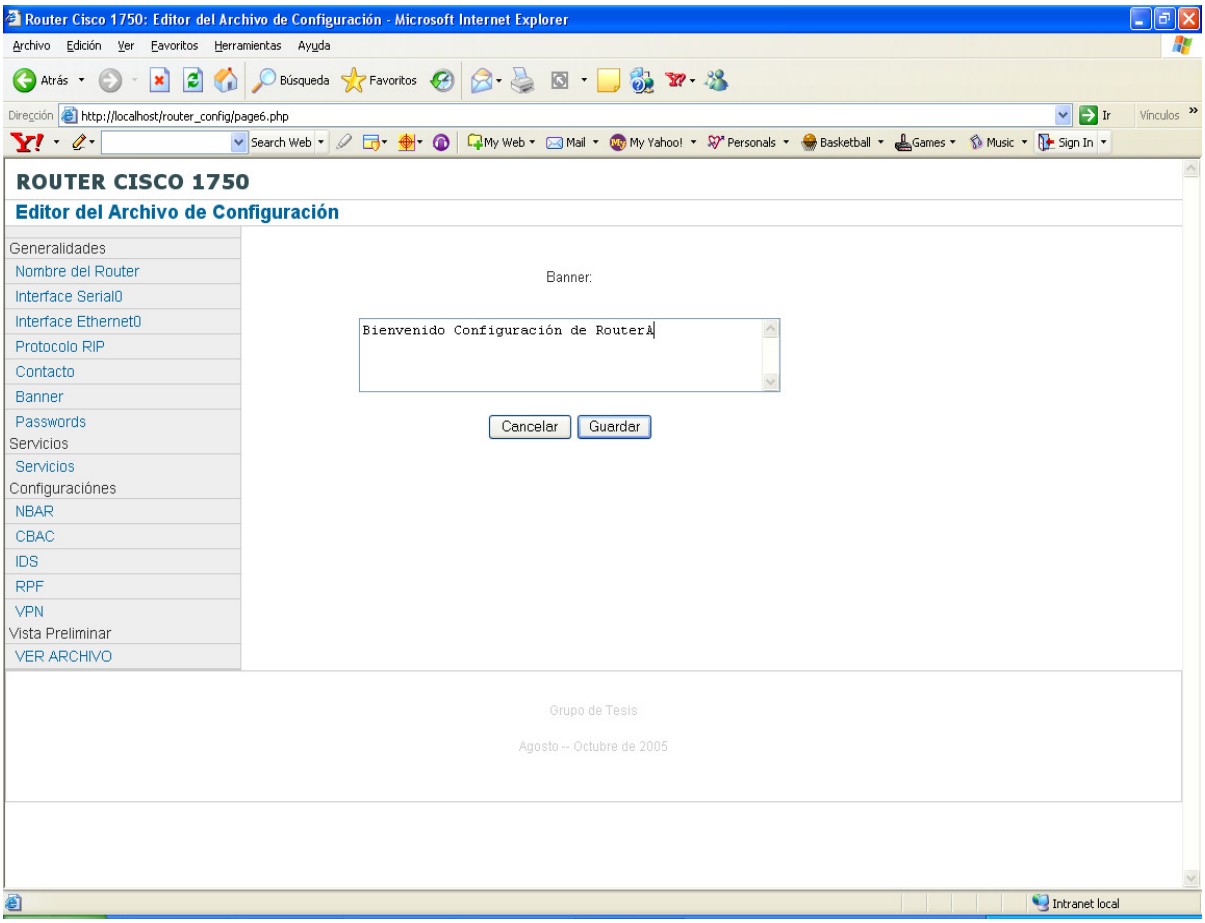


Figura A-6.10 Pantalla del software donde se detalla un mensaje de bienvenida a la consola de administración del router.

Al terminar de introducir todos los valores en la parte de generalidades se muestra una pantalla en la que aparece como mensaje “Fin de la Configuración de las Generalidades” si estas fueron realizadas con éxito.

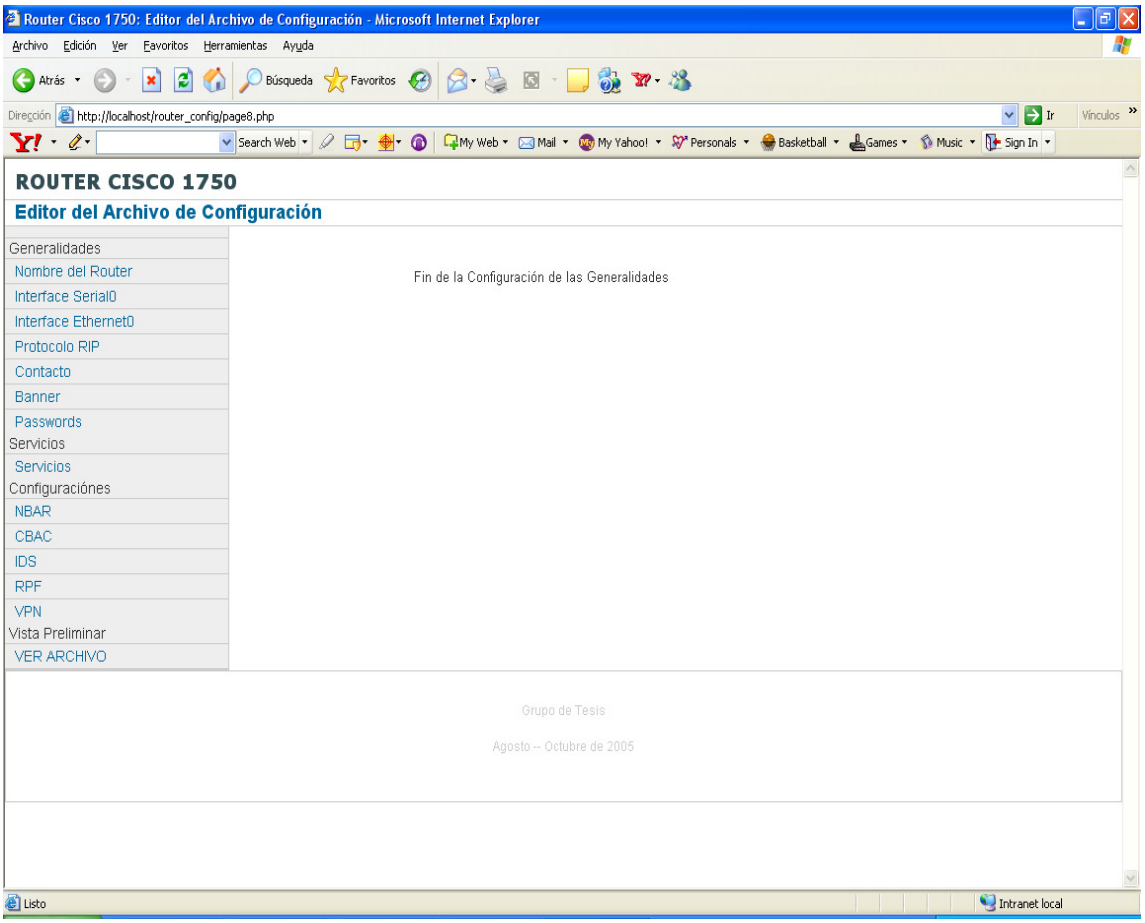


Figura A-6.11 Pantalla que muestra mensaje indicando éxito en la configuración de parámetros generales.

La segunda parte del software, presenta las opciones para configuración de servicios los cuáles al estar marcados con un cheque los habilita. En esta parte se pueden habilitar los servicios de:

- Service pad
- Service timestamps debug datetime msec
- Service timestamps log datetime msec
- Service password-encryption
- Service dhcp

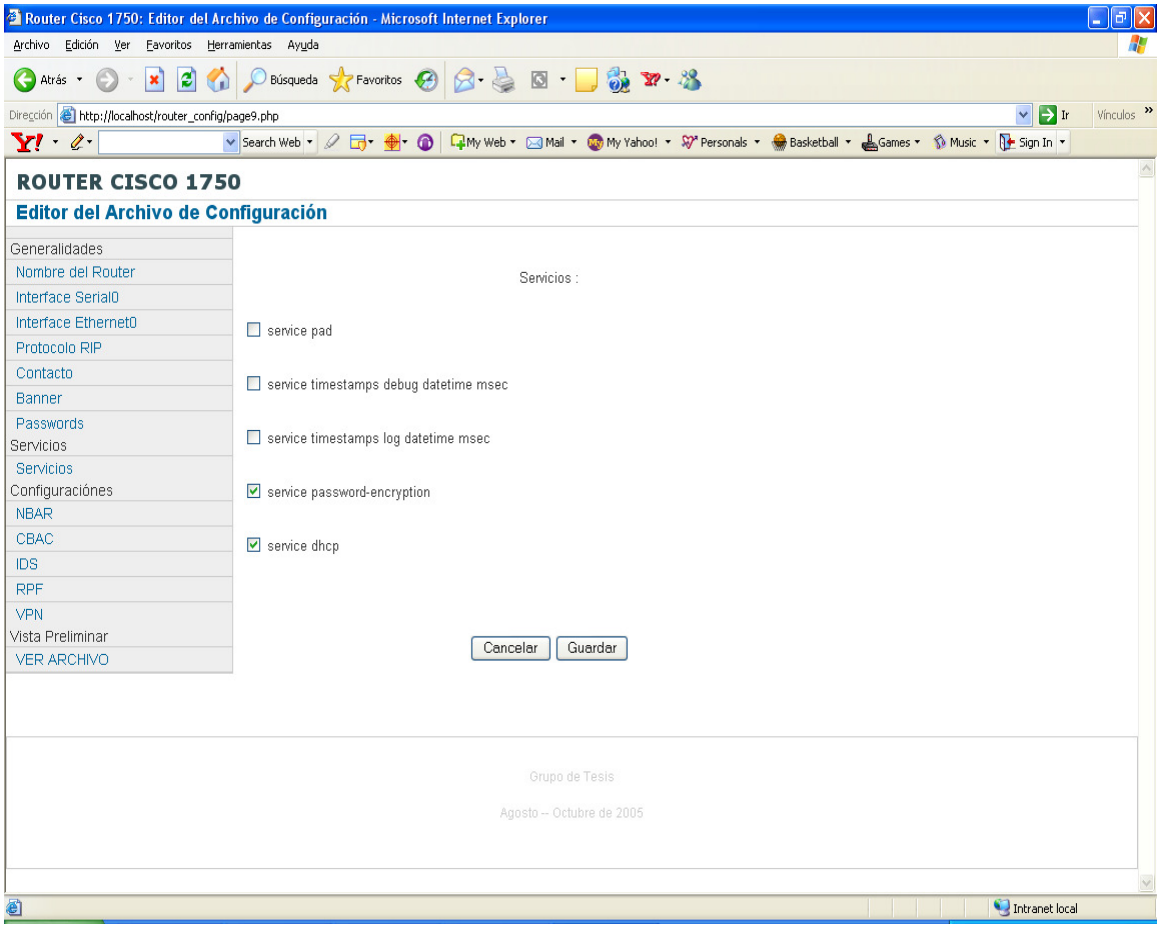


Figura A-6.12 Pantalla del software que permite habilitar o deshabilitar servicios en la configuración del router.

De igual manera como en todas las configuraciones, la de servicios presenta la ayuda emergente donde muestra una pequeña explicación sobre en que consiste cada servicio.

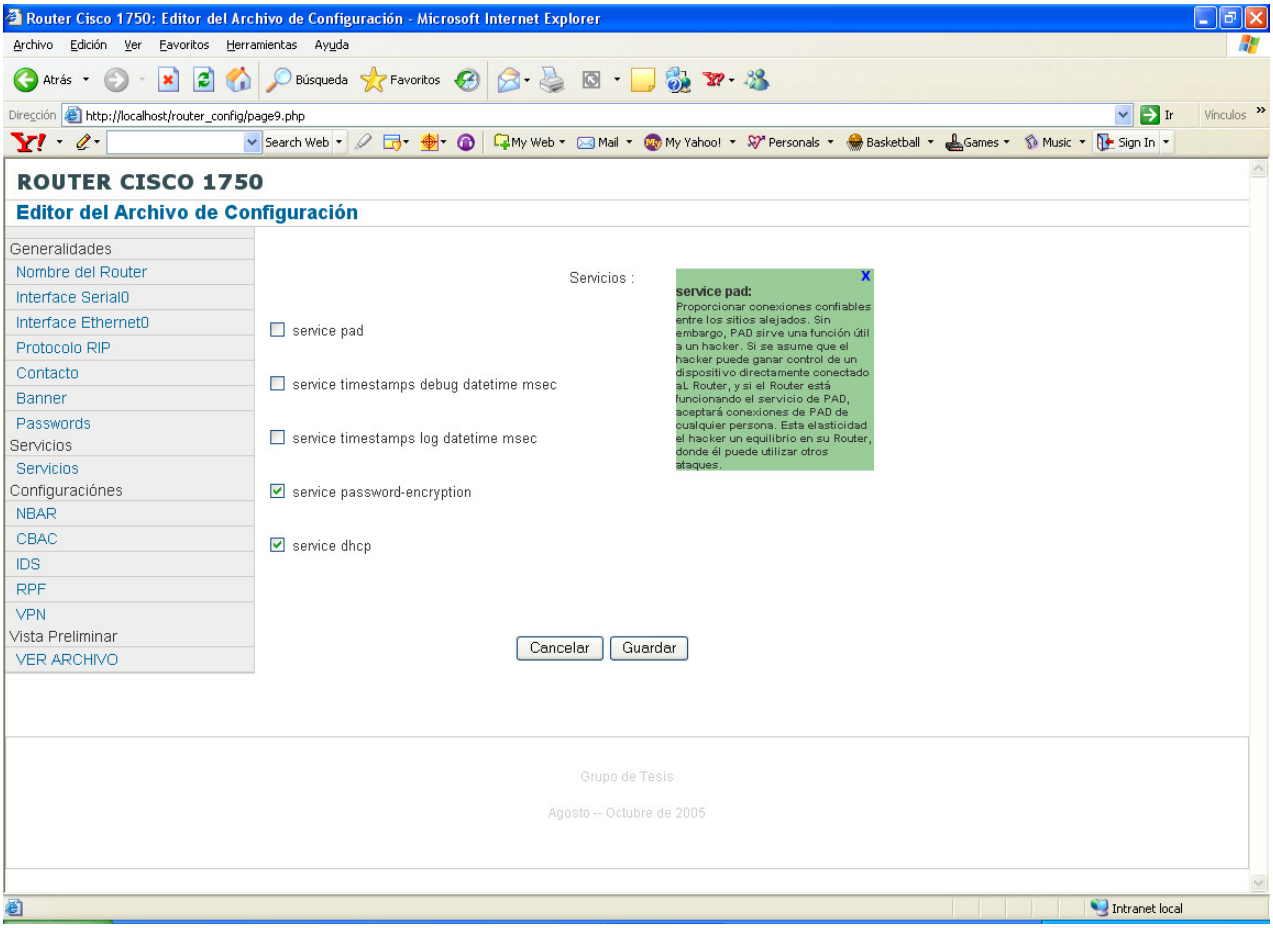


Figura A-6.13 Pantalla que muestra ayuda emergente del software.

Al terminar de introducir las opciones para la configuración de servicios, de haberlo hecho de manera correcta, muestra la siguiente ventana.

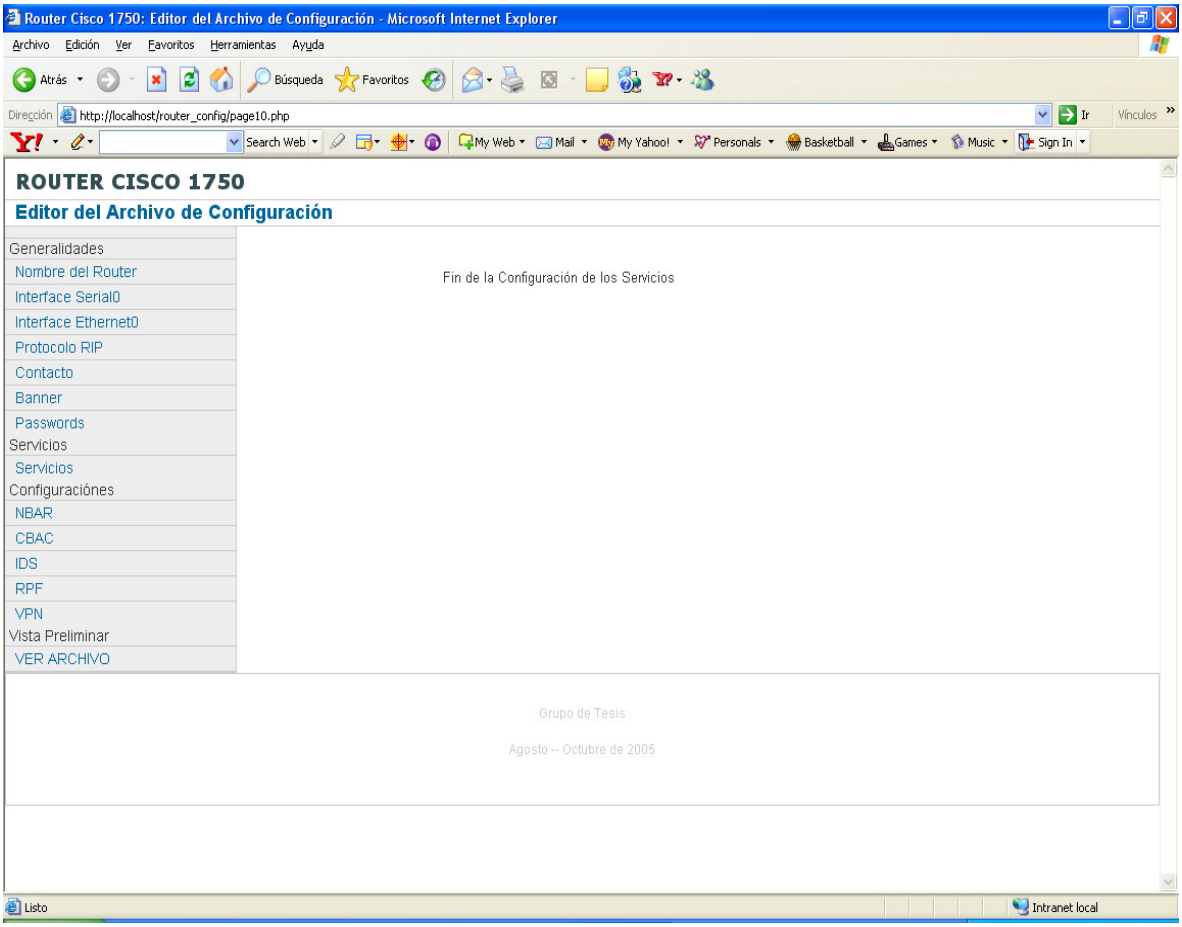


Figura A-6.14 Pantalla con mensaje indicando éxito en la configuración de servicios.

En la tercera parte de los parámetros a configurar se detallan las opciones para las técnicas a aplicar esta ventana muestra la de NBAR, donde se debe especificar un nombre, las condiciones, nombre de la política a crear, nombre de la acl, sentido en la que se aplicará la técnica en la interfaz serial o ethernet ya sea de entrada o salida.

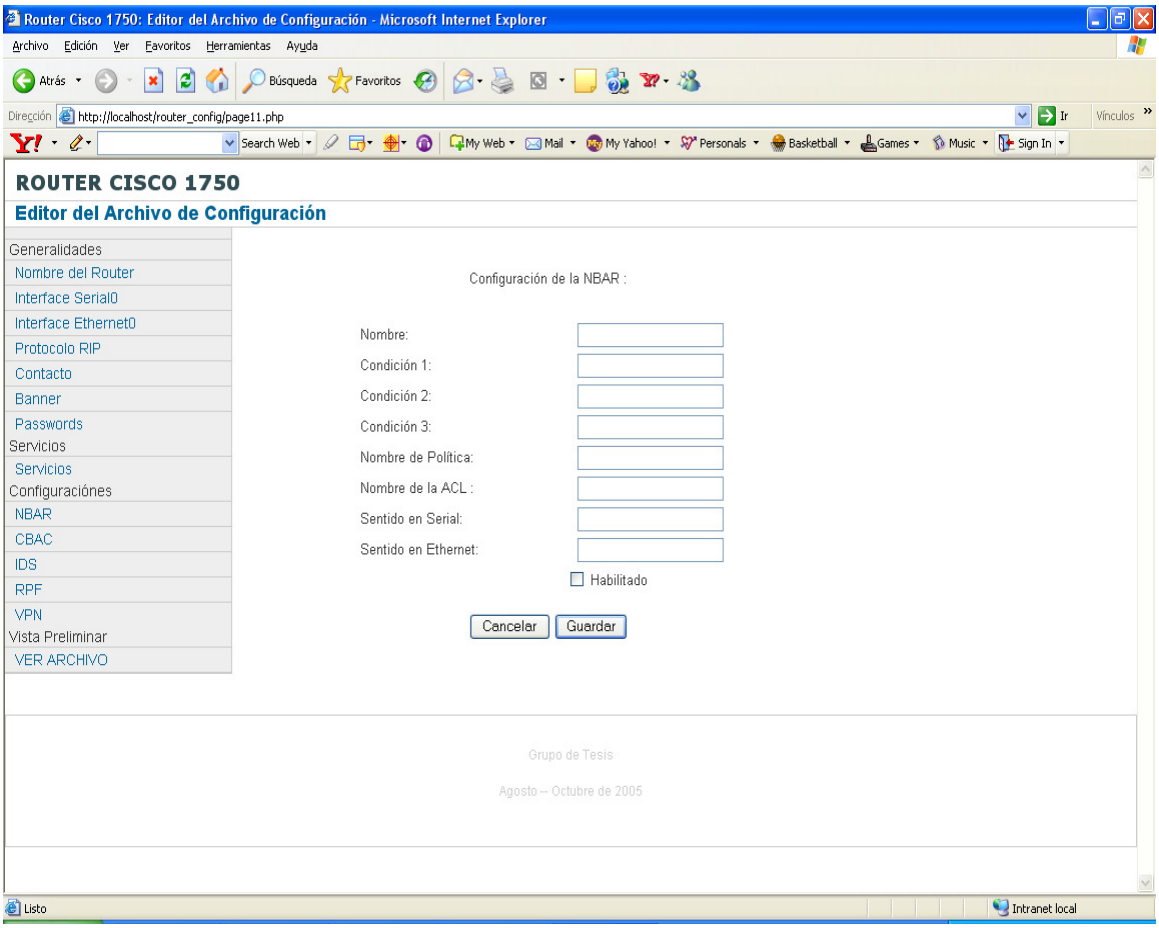


Figura A-6.15 Pantalla que muestra opciones a configurar en la técnica de NBAR.

Al finalizar la configuración de la técnica NBAR y de hacerlo de forma correcta se muestra una pantalla como la que se muestra a continuación.

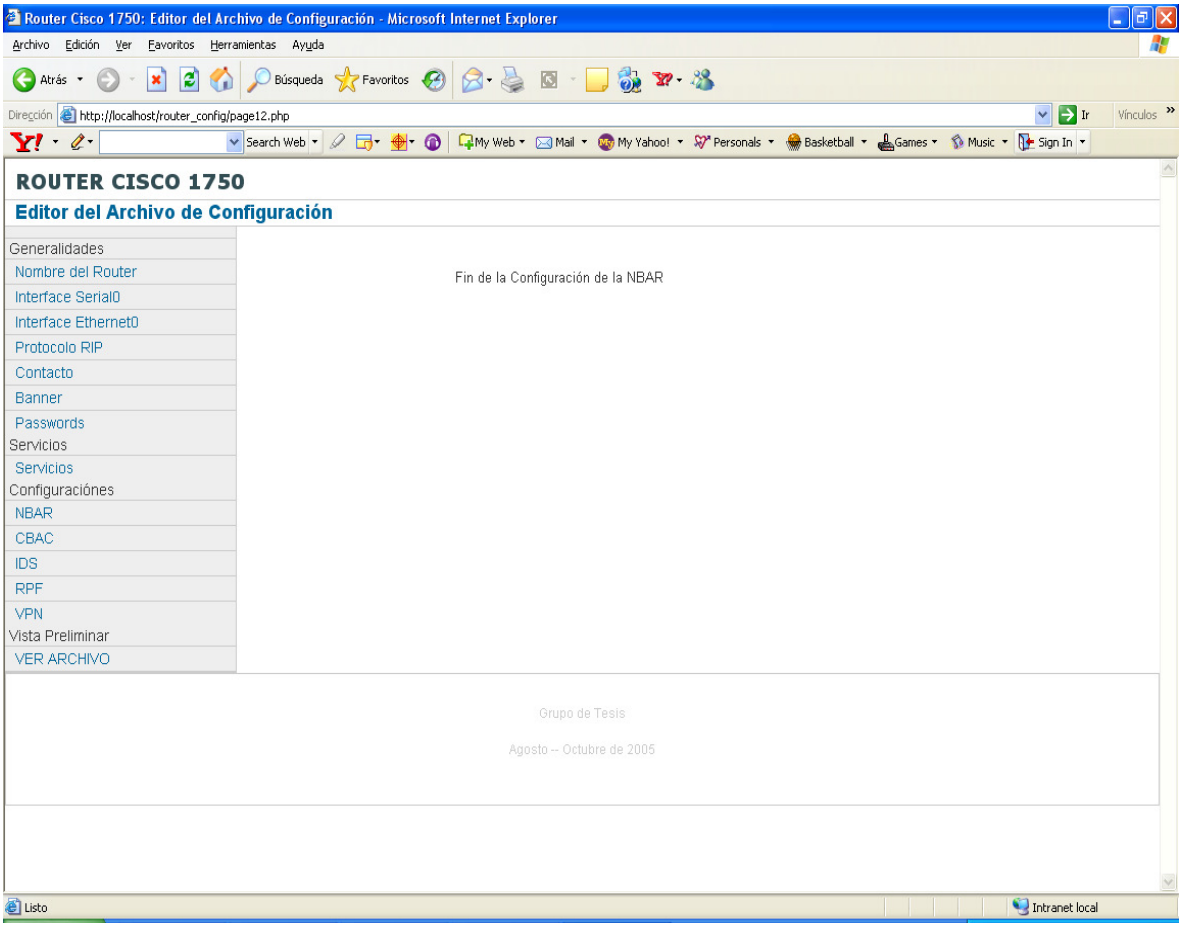


Figura A-6.16 Pantalla que muestra mensaje indicando éxito en configuración de técnica de NBAR.

En la técnica de IDS, se deben tomar en cuenta los siguientes parámetros:
IP de rango 1, IP de rango 2, Información de alarma de acción, Alarma de acción de ataque, Sentido de la IDS en la interface serial (ya sea de entrada o de salida).

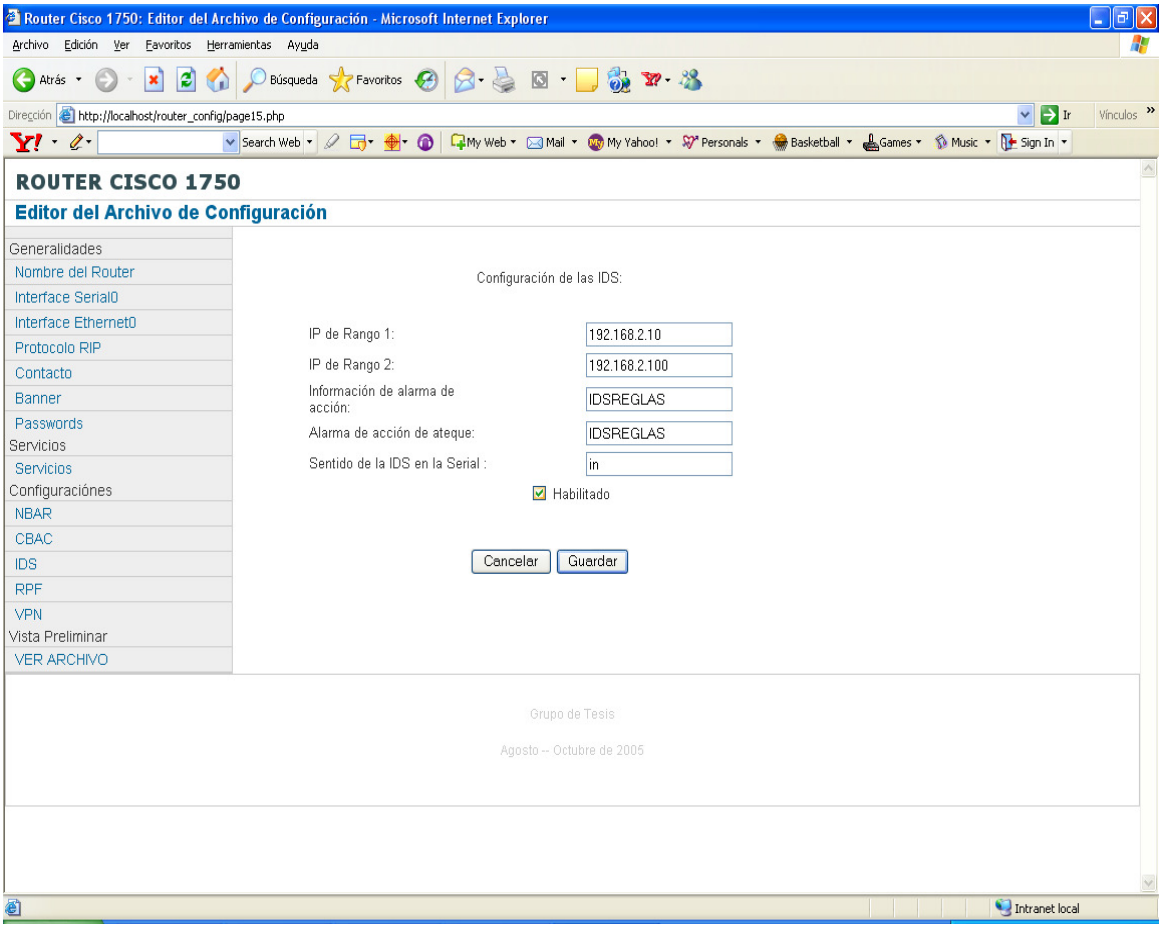


Figura A-6.17 Pantalla que muestra opciones de configuración de técnica IDS.

Al concluir de ingresar bien los valores de configuración de IDS se muestra la siguiente pantalla.

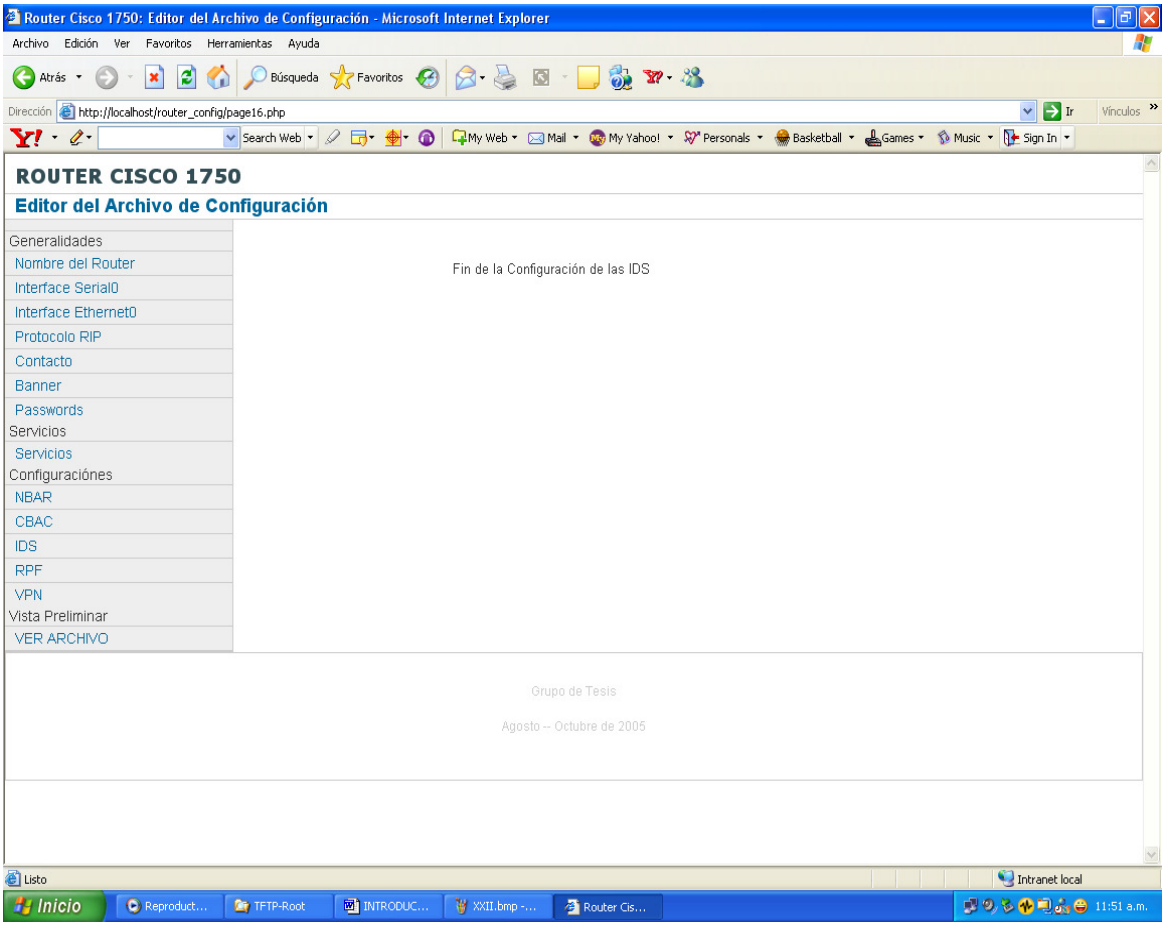


Figura A-6.18 Pantalla con mensaje indicando éxito en la configuración de la técnica IDS.

En la técnica de RPF se especifican los valores de: Nombre de la ACL, IP permitida 1, IP permitida 2.

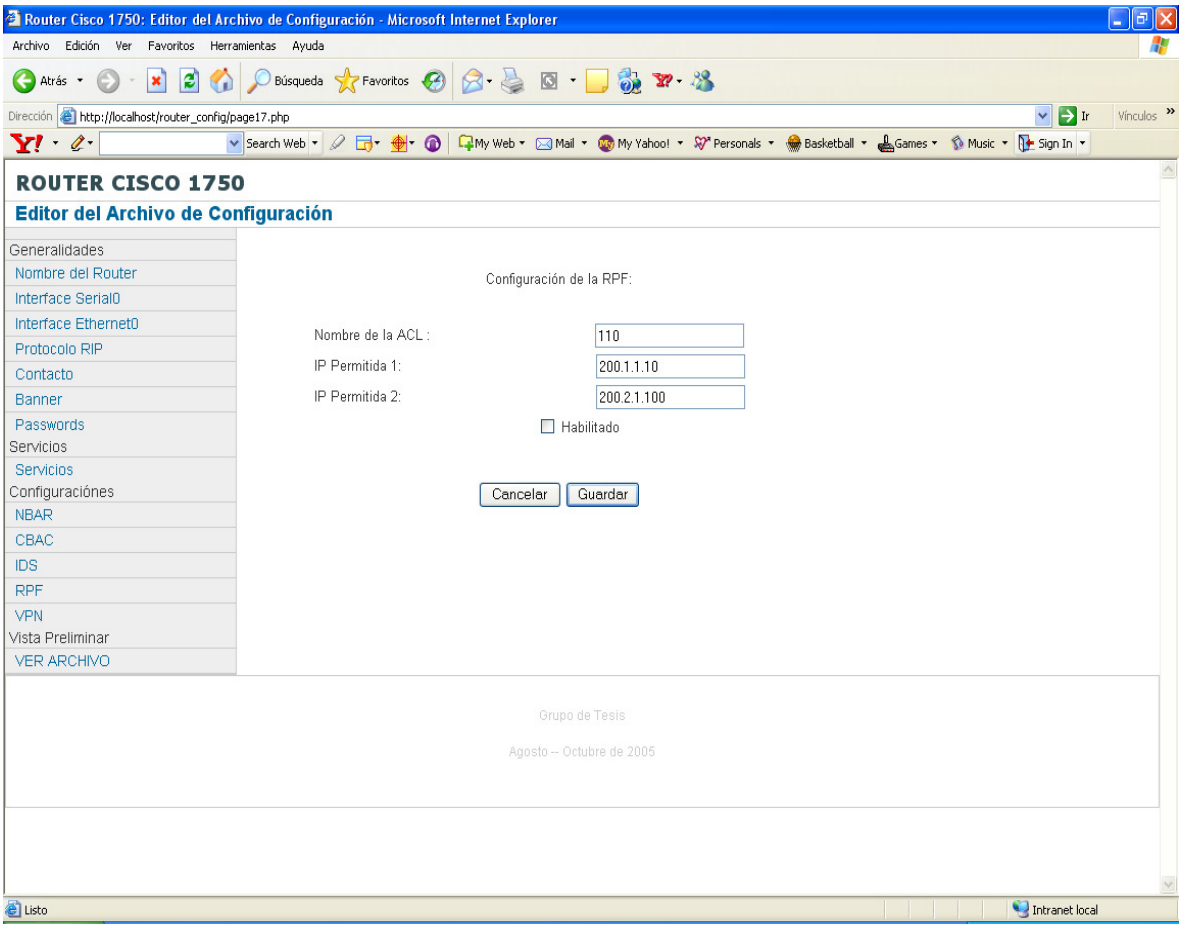


Figura A-6.19 Pantalla que muestra parámetros de configuración en la técnica de RPF.

Al concluir de configurar las opciones para la técnica RPF y de haberlo hecho de manera correcta se muestra una pantalla como la siguiente:

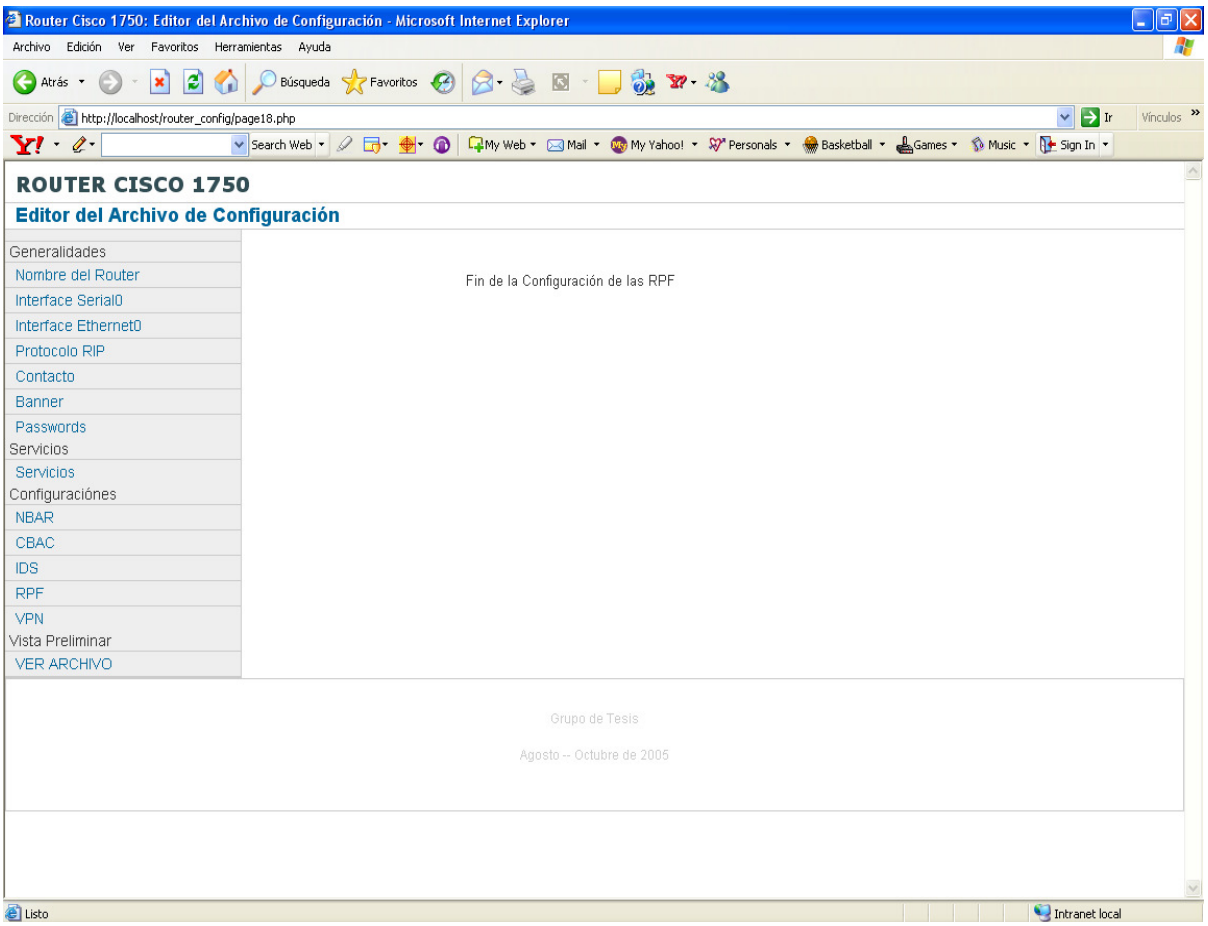


Figura A-6.20 Pantalla con mensaje indicando éxito en la configuración de técnica RPF.

La siguiente pantalla muestra la configuración de la VPN detallando cada uno de los campos:

Nombre de la VPN: se digita el nombre de la VPN este mismo nombre debe de digitarse en el otro router donde se configurarála VPN.

IP del otro router: Dirección IP de la interface del otro router con la que se construiráel túnel virtual. Este puede ser la interface serial o ethernet.

Número de política: políticas de seguridad que se aplican al tráfico deseado

Nombre de la llave: se intercambia en la negociación inicial, es necesario configurarla en cada extremo.

IP Interface en otro router: Se da la dirección IP del host destino.

Habilitado: Se chequea, si se quiere habilitar la configuración creada.

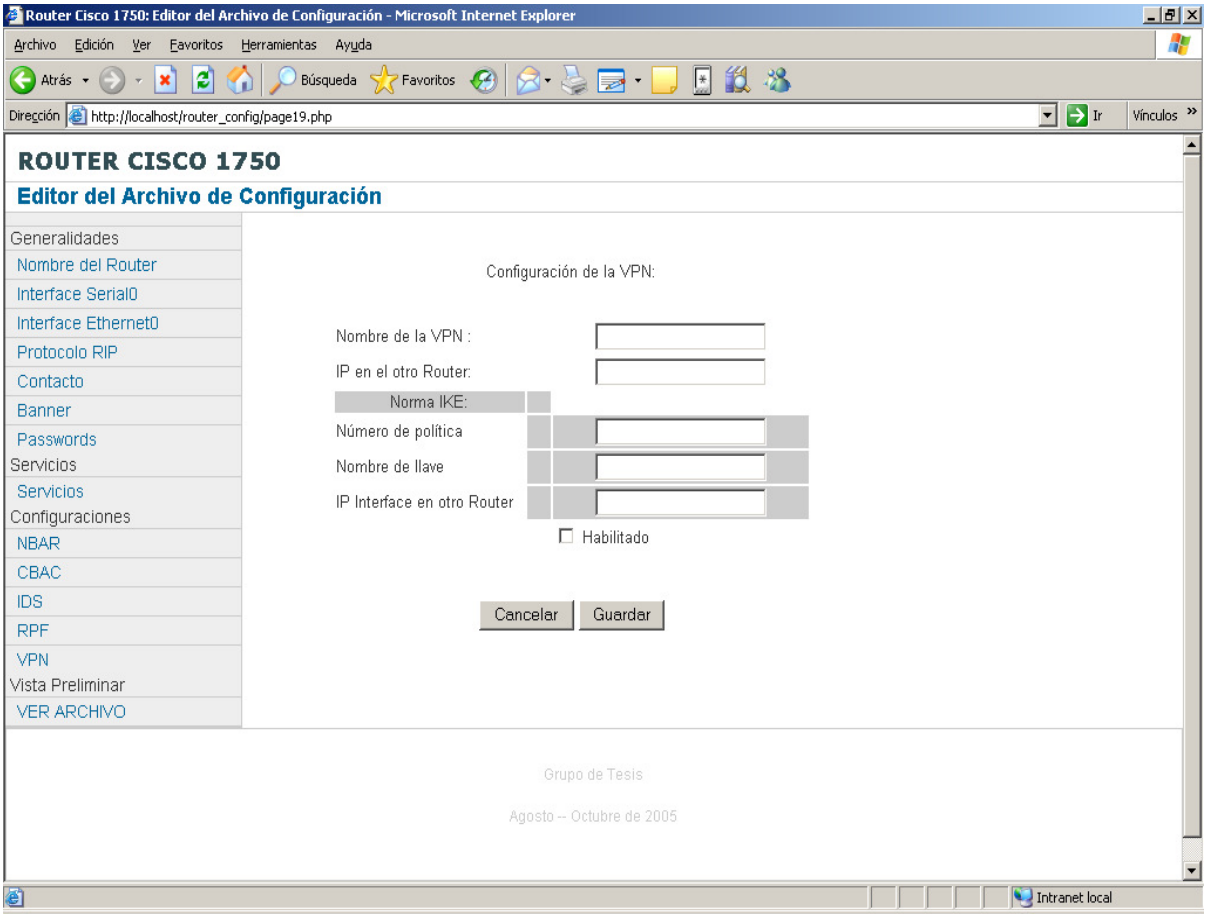


Figura A-6.21 Pantalla que muestra opciones de configuración de la VPN.

Cuando se concluye con los valores asignados a cada técnica se puede ver de forma preliminar el archivo de configuración que se carga en el router en la última opción del menú en Vista Preliminar se debe posicionar sobre el botón VER ARCHIVO y luego presionamos, presentando la siguiente.

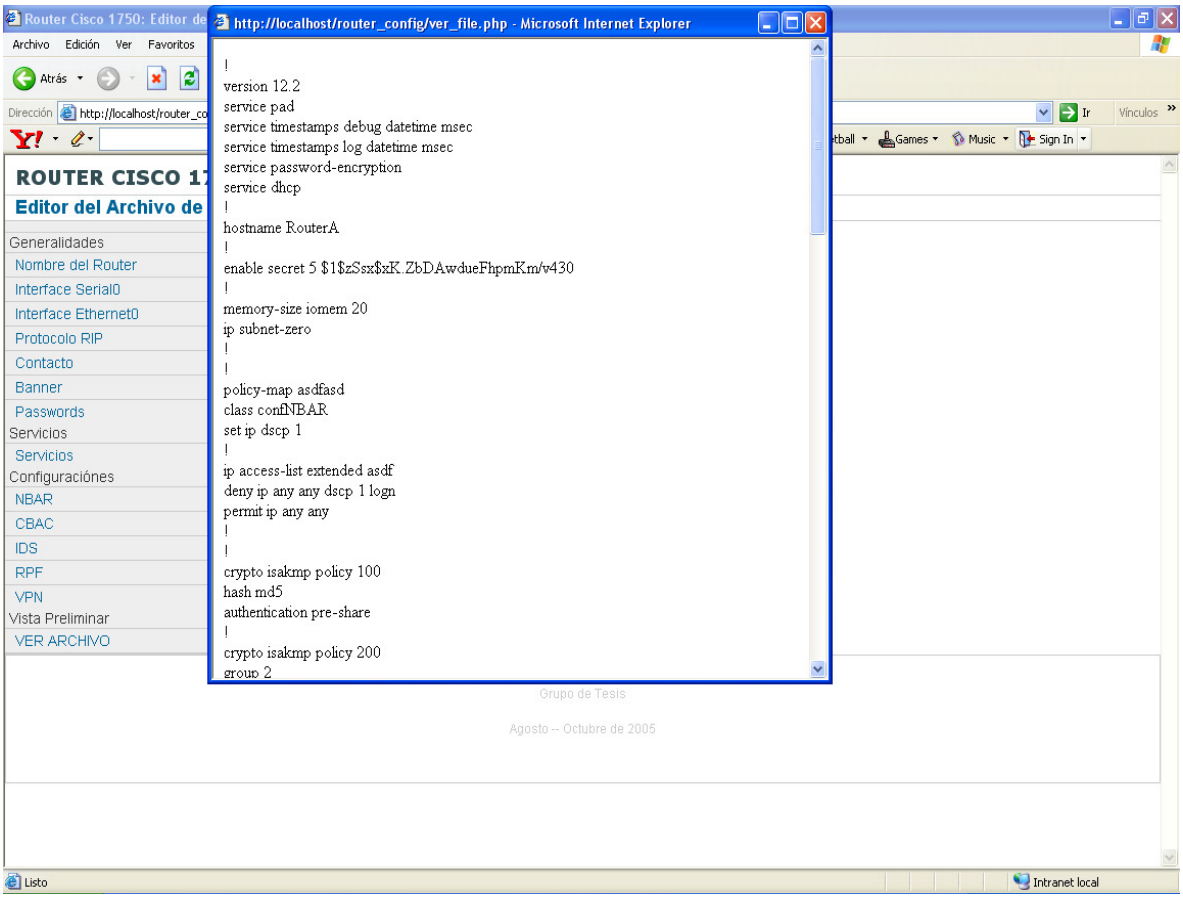


Figura A-6.22 Pantalla que detalla una vista preliminar de archivo de configuración de router.

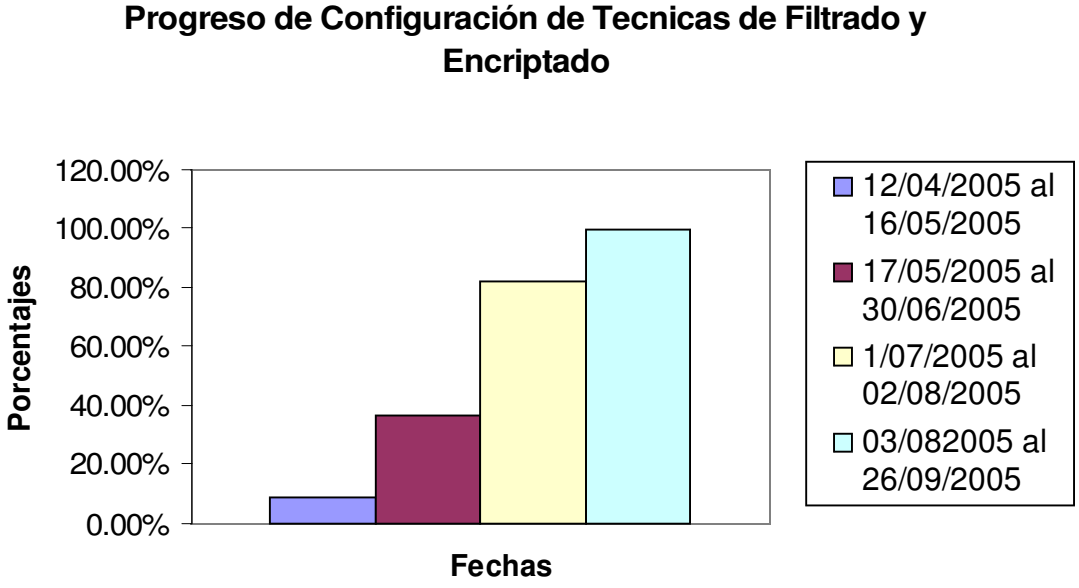
ANEXO 7. PROGRESO EN CONFIGURACIÓN DE TÉCNICAS

La siguiente tabla muestra el progreso de las diferentes técnicas que se utilizaron para la configuración del Router Cisco 1750

FECHA	NBAR	CBAC	RPF	RATE LIMIT	IDS	BLACK HOLE	AP	VPN	FAILOVER	NAT	URL FILTERING
12/04/2005 al 16/05/2005											
17/05/2005 al 30/06/2005											
1/07/2005 al 02/08/2005											
03/082005 al 26/09/2005											

Tabla A-7.1 Periodos de demostración de la diferentes técnicas de encriptado y filtrado.

En proceso Finalizado



La gráfica muestra el porcentaje de progreso de la configuración de las distintas técnicas que se utilizaron para que el Router cumpliera la función de Firewall:

- Para el período comprendido del 12/04/2005 al 16/05/2005 se había realizado la configuración en un 9% del total de las técnicas a probar. Solamente se logróconfigurar RPF.

- Entre el período del 17/05/2005 al 30/06/2005 se avanzó a un 36.36% de la ejecución con las técnicas siguientes: IDS,VPN, NAT.

- Para el período del 1/07/2005 al 02/08/2005 un avance del 81.8% del total de técnicas a comprobar. Se concluyeron las pruebas correspondientes a NBAR, CBAC, Rate Limit, Black Hole y URL Filtering.

- Se finalizo la configuración en el periodo del 03/08/2005 al 26/09/2005 de las siguientes técnicas AP y la configuración de respaldo de conexión Failover.

Estadísticas de Pruebas de Ataques.

La siguiente tabla muestra el número de intentos o pruebas tanto fallidas como satisfactorias de los diferentes ataques o vulnerabilidades realizados:

Ataque o Vulnerabilidades	Número de Pruebas	Pruebas Fallidas	Pruebas Satisfactorias	Técnica Implementada	Porcentaje de Pruebas Fallidas	Porcentaje de Pruebas Satisfactorias	Fecha de Finalización
DDoS (UDP echos,SmurfTCP SYN flooding)	**10**	4	6	Rate Limiting	40.00%	60.00%	02/08/2005
DDoS	**7**	3	4	NBAR	42.86%	57.14%	02/08/2005
Tráfico no deseado (Solicitudes de orígenes no permitidos)	**10**	5	5	Black Hole	50.00%	50.00%	02/08/2005
Spoofing	**5**	2	3	RPF	40.00%	60.00%	16/05/2005
Accesos no Autorizados	**10**	4	6	Autenticación Proxy	40.00%	60.00%	26/09/2005
PING OF DEATH (DoS)	**4**	1	3	CBAC	25.00%	75.00%	02/08/2005
Traslación de direcciones privadas a públicas	**4**	1	3	NAT	25.00%	75.00%	30/06/2005
Detección de Intrusos	**6**	2	4	IDS	33.33%	66.67%	30/06/2005
Problemas de Redundancia	**10**	2	8	Failover	20.00%	80.00%	26/09/2005
Conexión Segura	**5**	2	3	VPN	40.00%	60.00%	30/06/2005
Integridad de Información	**4**	1	3	IPSec (DES, MD5)	25.00%	75.00%	30/06/2005
Sitios Web prohibidos	**10**	3	7	URL Filtering	30.00%	70.00%	26/09/2005
Total de pruebas	**85**	**30**	**55**				
Porcentaje de pruebas		**35.29%**	**64.71%**				

Tabla A-7.2 Estadísticas de pruebas fallidas y exitosas de ataques realizados.

Análisis de las Pruebas realizadas:

En la tabla A- 7.2 correspondiente a las pruebas de ataques realizados, se presentan los datos concernientes al número total de pruebas hechas por cada uno de los ataques, además se presenta la técnica utilizada para tratar de prevenir dicho ataque.

En la columna de número de pruebas se muestran el número total de intentos realizados por ataque y por técnica, también en la columna pruebas fallidas se presentan los datos correspondientes a cuántas veces el ataque no fue detenido y en la columna de prubas satisfactorias cuántas veces hubo el ataque fue detenido.

En la tabla A- 7.1 se muestran los períodos en los cuales se implementaron las técnicas, es de mencionar que desde el principio de la implementación de cada técnica se realizaron ataques, inicialmente el ataque lograba su objetivo, para lo cual se modificaban parámetros de configuración de tal forma que se puediera identificar la falla en la configuración realizada, con el propósito de detener el ataque.

En tabla de datos A- 7.2 se puede observar a cabalidad cuántas veces se logró realizar el ataque como tal es de hacer la aclaración que los números corresponden al número de intentos. Por ejemplo si se observa que para Sitios Web prohibidos se realizaron un total de 10 intentos, los primeros 3 intentos o ataques fueron concretados y los siguientes 7 fueron rechazados por la técnica URL Filtering. De esta misma forma puede irse interpretando cada uno de los datos contenidos en la tabla.

Como dato adicional, las pruebas fueron secuenciales, es decir que si existieron 5 intentos fallidos y 5 intentos satisfactorios se debe a que en el período en el que se configuró dicha técnica, hubieron 10 intentos, los primeros 5 ataques fueron fallidos y los siguientes 5 fueron detenidos por la técnica. Estos se detallan porcentatualmete en la tabla A- 7.2 donde se observa que el porcentaje de pruebas fallidas es de 35.29% y el de pruebas satisfactorias asciende a 64.71% del total de pruebas

hechas. Al finalizar las pruebas se logró detener en un 100% todos los ataques o vulnerabilidades que se realizaron.

ANEXO 8. MANUAL DE CONFIGURACION DE APACHE Y PHP

Pasos de Instalación del software de Configuración del Router 1750

- Instalación del Apache

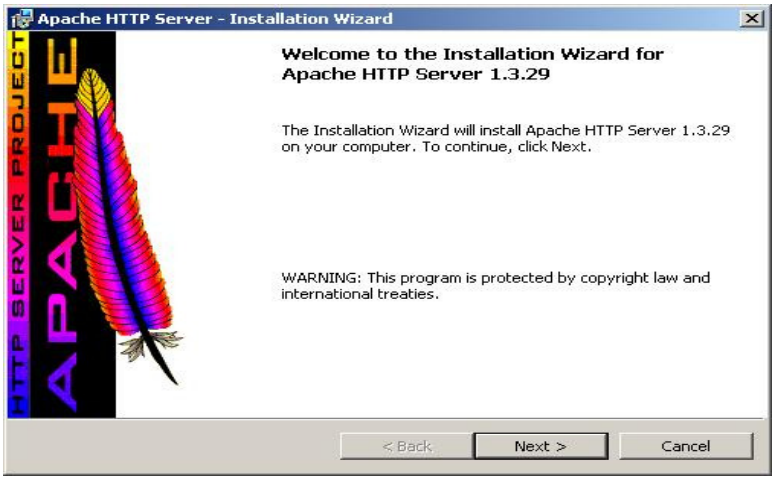


Figura A-8.1 Pantalla de inicio de instalación del apache, se debe posicionar sobre el el botón Next y presionamos.

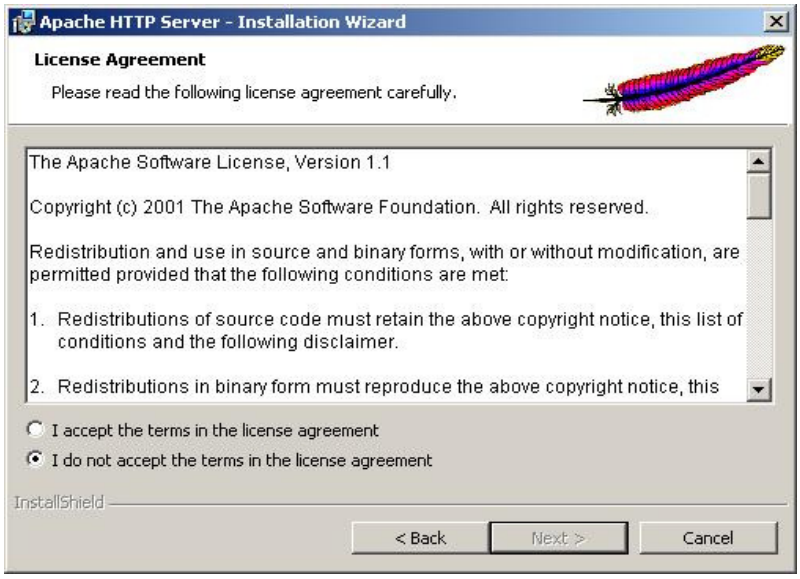


Figura A-8.2 En esta pantalla damos ser realiza dos acciones primero aceptamos los términos de la licencia y posteriormente se debe posicionar sobre el el botón Next y presionamos.

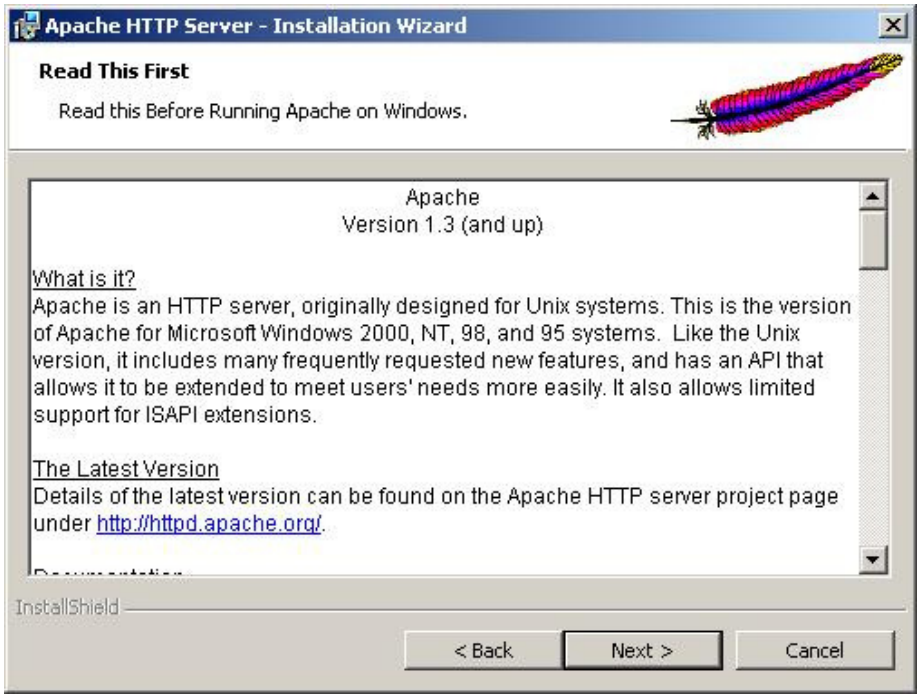


Figura A-8.3 Para continuar con la instalación se debe posicionar sobre el el botón Next y presionamos.

.

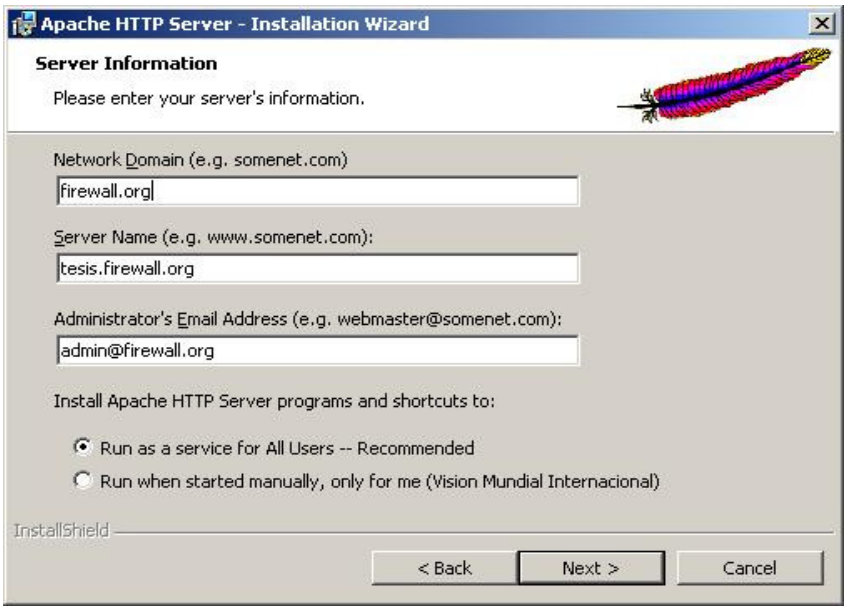


Figura A-8.4 En esta pantalla digitamos la información requerida para la configuración del servidor, luego se debe posicionar sobre el el botón Next y presionamos. (Ejemplo se muestra en la ventana de configuración).

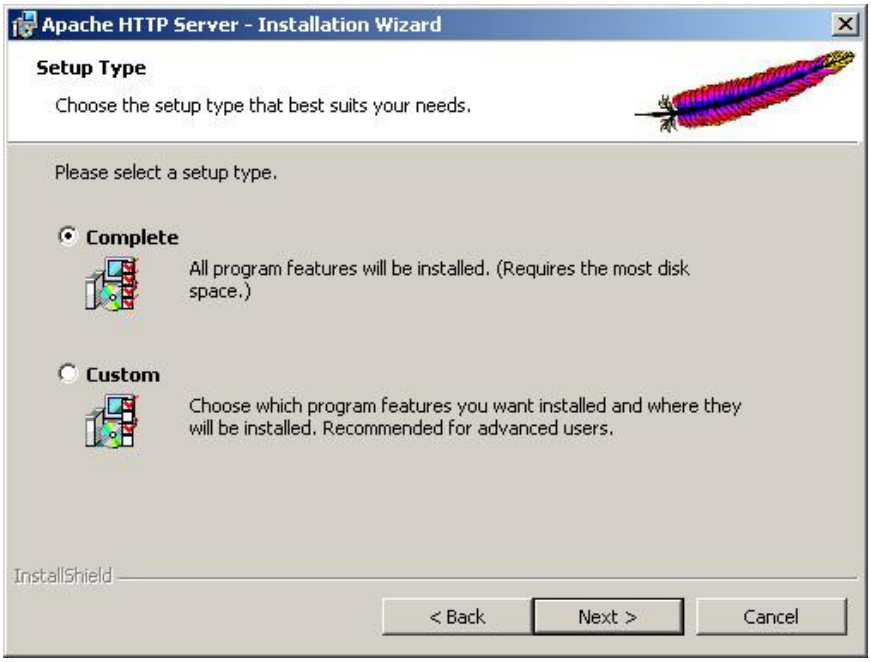


Figura A-8.5 Luego escogemos el tipo de instalación. Para nuestro caso será completa. Se debe posicionar sobre el el botón Next y presionamos.

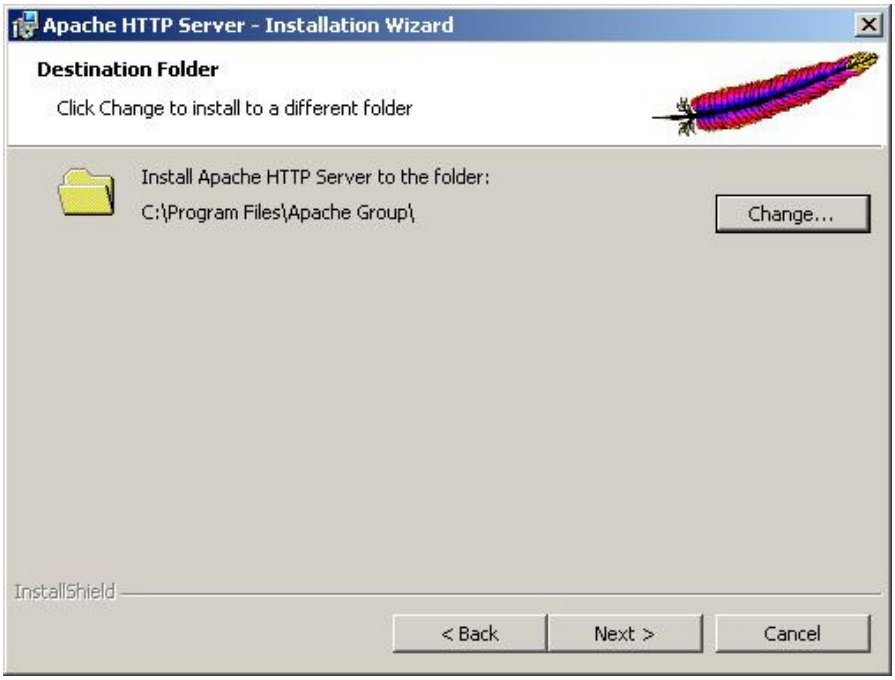


Figura A-8.6 En esta pantalla definiremos la carpeta donde se instalará el Apache, luego nos posicionamos sobre el botón Next y presionamos.

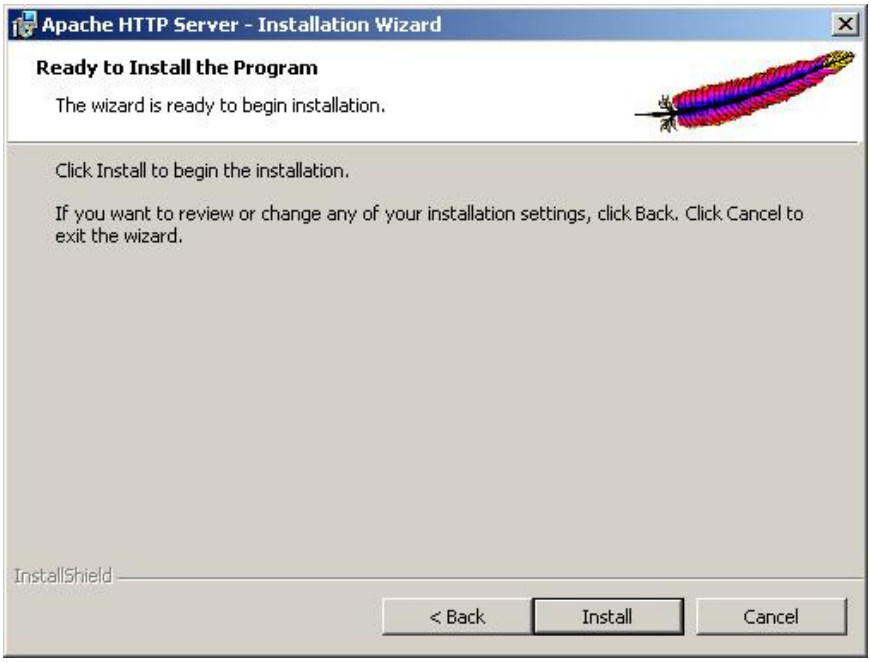


Figura A-8.7 Luego de terminar de configurar la información básica iniciamos el proceso de instalación de Apache posicionándonos sobre el botón Install y presionando.

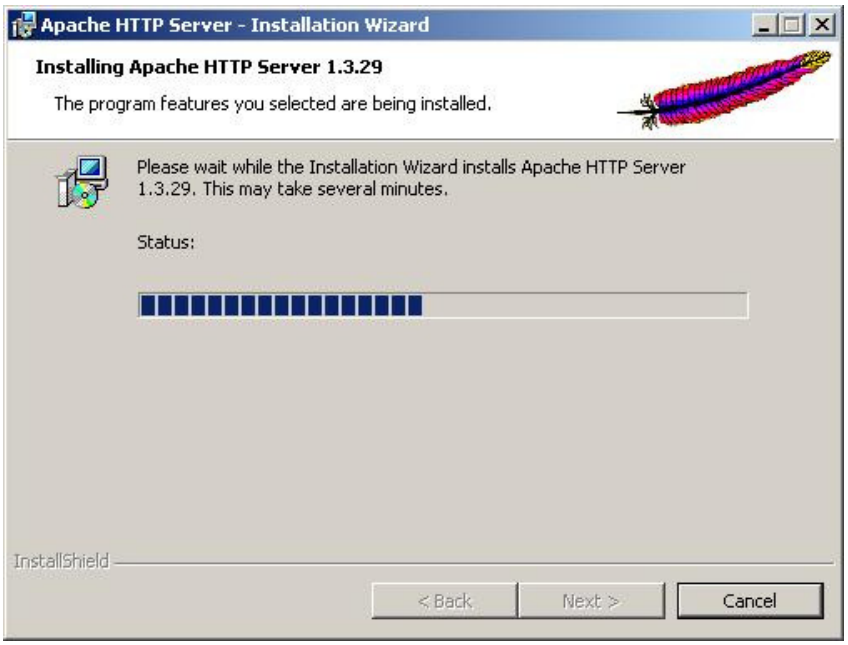


Figura A-8.8 Esta pantalla muestra el progreso de instalación.

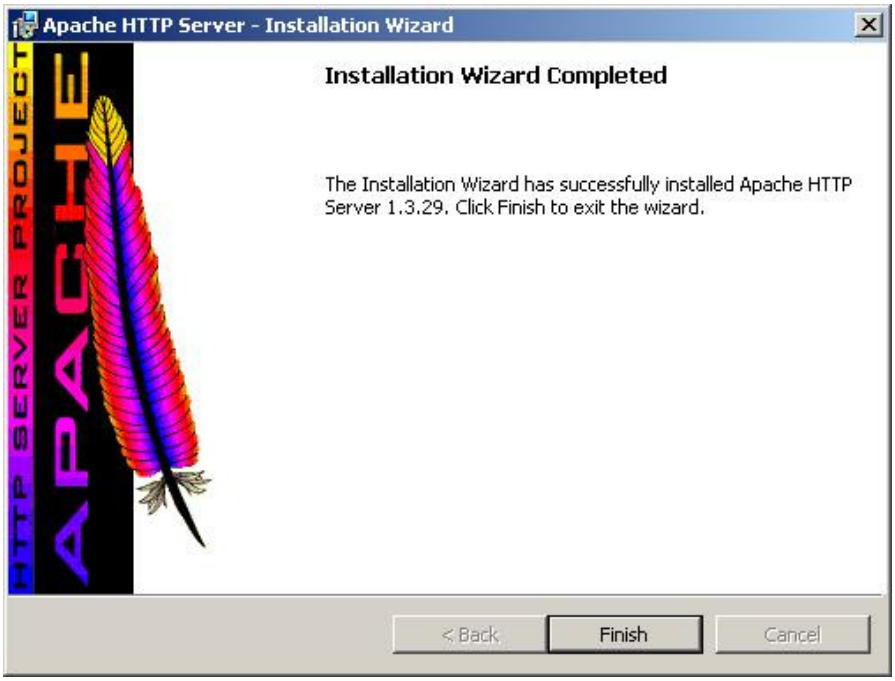


Figura A-8. 9 Luego de finalizado el proceso posicionándonos sobre el botón Finish y presionando.

.

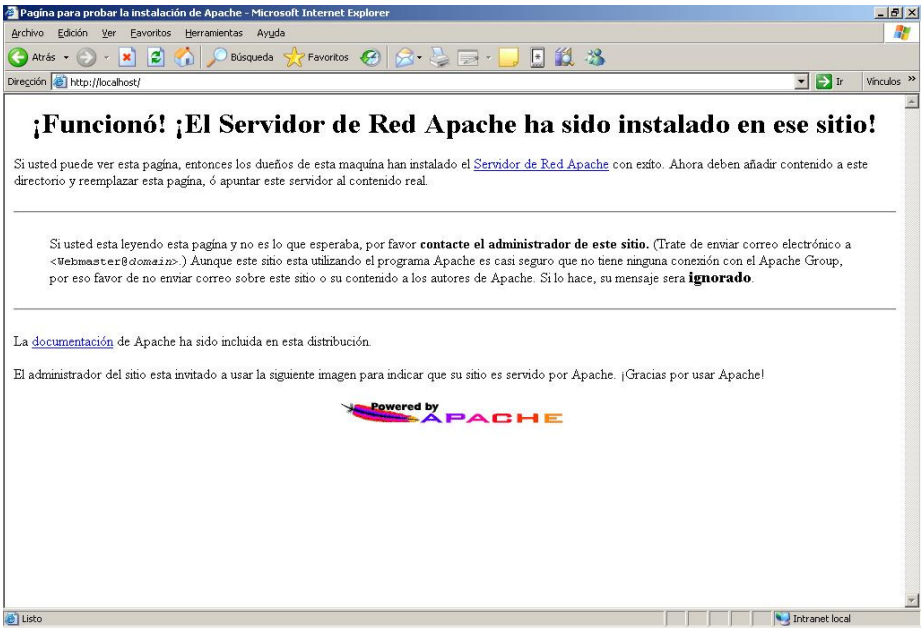


Figura A-8.10 Para comprobar si se ha instalado correctamente el Apache digitamos en el explorador la siguiente dirección. http://localhost/. El resultado tendría que ser la pantalla anterior. Donde se muestra el buen funcionamiento del servidor Apache.

- **Instalación de PHP**

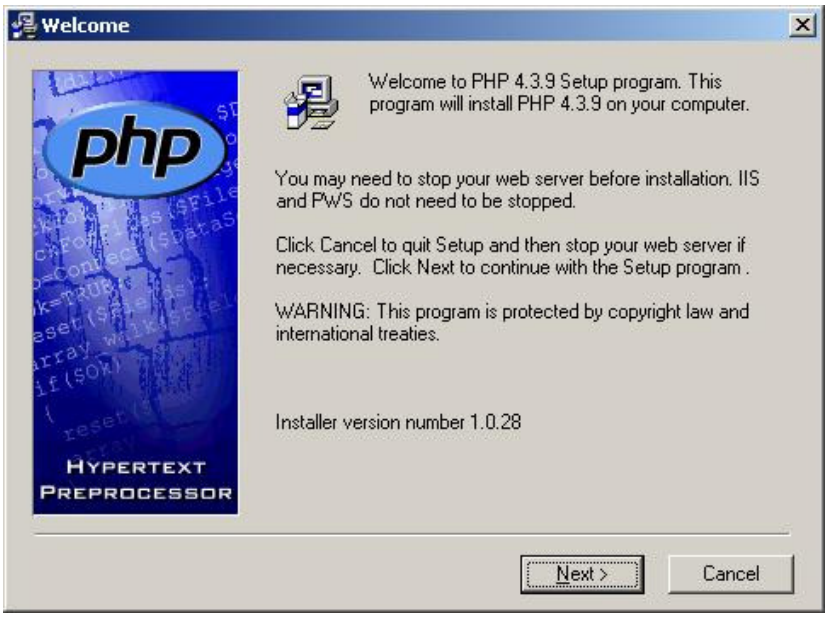


Figura A-8.11 Pantalla de bienvenida a la instalación de PHP, se debe posicionar sobre el el botón Next y presionamos.

.

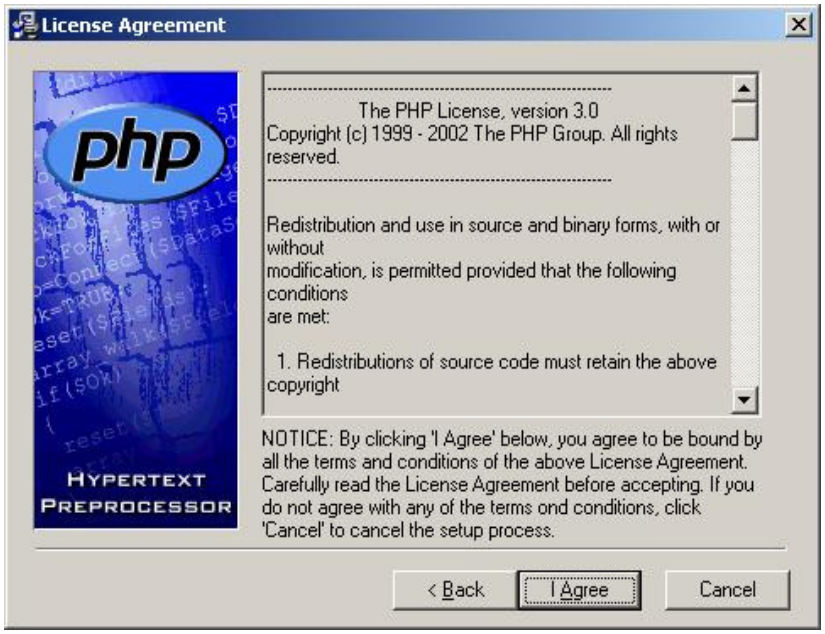


Figura A-8.12 Luego aceptamos la licencia posicionándonos sobre el botón I Agree y presionamos.

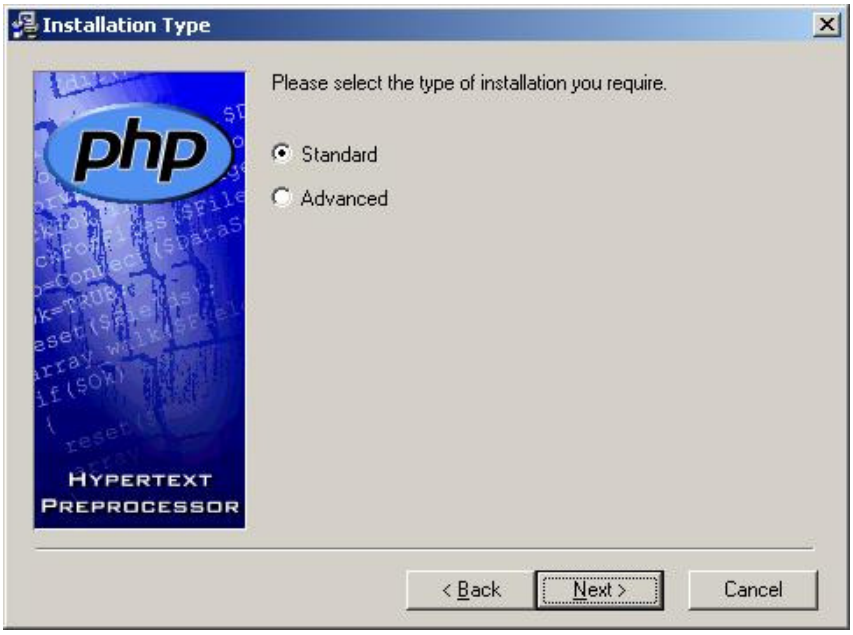


Figura A-8.13 Escogemos el tipo de configuración Standard y luego se debe posicionar sobre el el botón Next y presionamos.

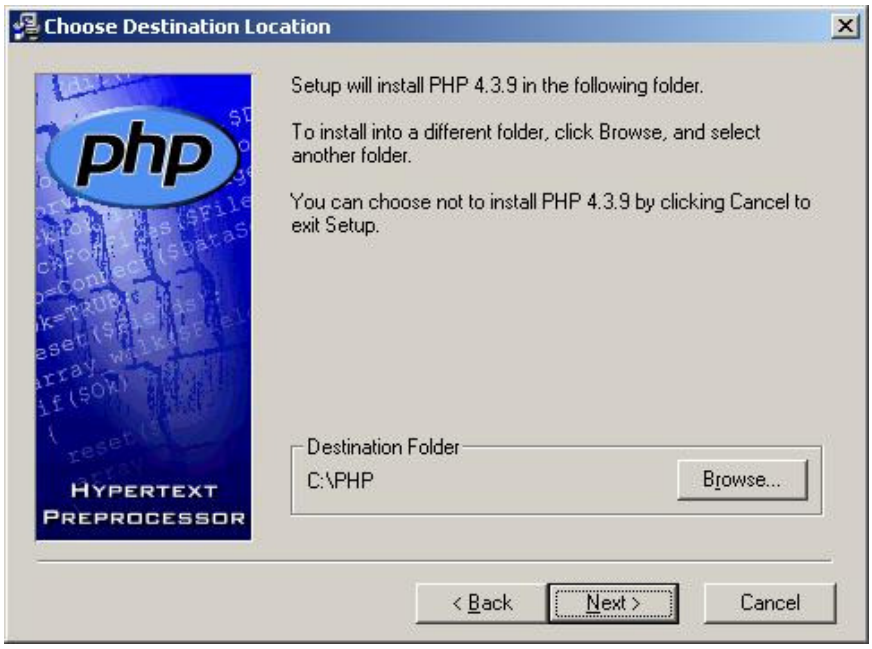


Figura A-6.14 Luego escogemos la ruta donde se instalara el PHP y nos posicionamos sobre el botón Next y presionamos.

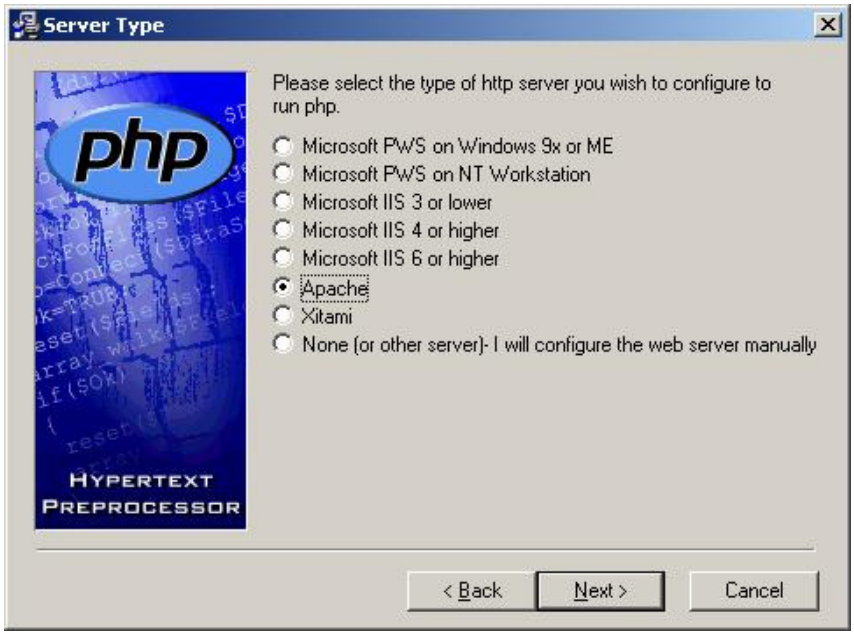


Figura A-8.15 Escogemos como servidor Web que en nuestro caso será el Apache, luego se debe posicionar sobre el el botón Next y presionamos.

.

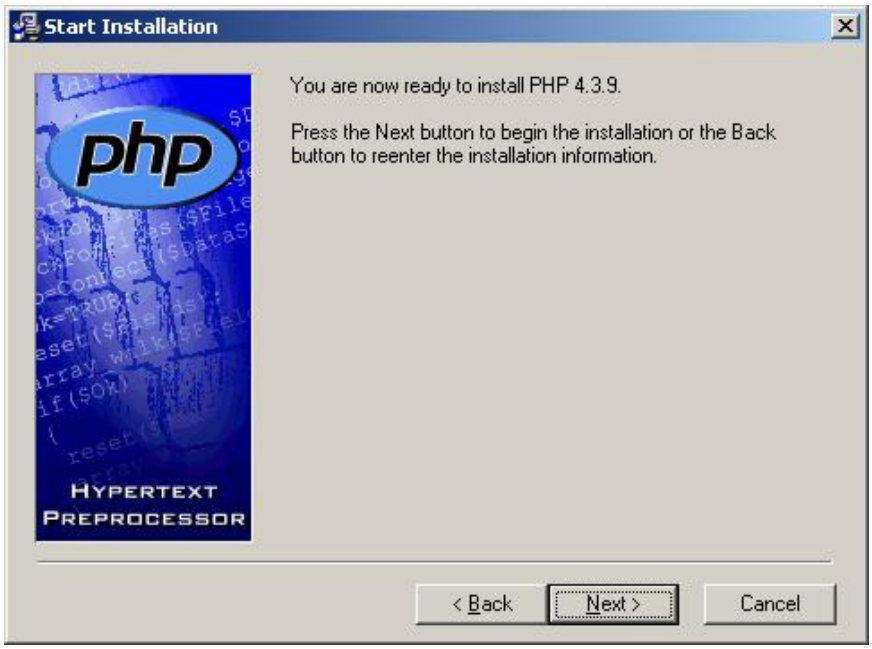


Figura A-8.16 Se debe posicionar sobre el el botón Next y presionamos, para iniciar el proceso de instalación del PHP.

Figura A-8.17 Esta pantalla muestra el progreso de la instalación.

Figura A-8.18 Pantalla que indica que la instalación a terminado satisfactoriamente.

- Finalmente copias la carpeta Apache Group que se encuentra en el CD anexo dentro de la carpeta Instaladores. Y la pegamos en el disco duro en la

siguiente carpeta C:\Program Files. Si nos pregunta si deseamos sobre escribir algunos archivos le decimos que si.