UNIVERSIDAD DON BOSCO
FACULTAD DE INGENIERÍA
ESCUELA DE ELECTRÓNICA

TRABAJO DE GRADUACIÓN
PARA OPTAR AL TITULO DE
INGENIERO EN TELECOMUNICACIONES

DESCRIPCIÓN, COMPROBACIÓN DEL FUNCIONAMIENTO Y DE LAS APLICACIONES DISPONIBLES DE DISPOSITIVOS UTM (UNIFIED THREAT MANAGEMENT).

PRESENTADO POR:
JUAN ANTONIO GARCÍA RENDEROS

ASESOR:
ING. FRANCISCO ROBLES

SEPTIEMBRE 2008
EL SALVADOR CENTRO AMERICA

UNIVERSIDAD DON BOSCO
FACULTAD DE INGENIERÍA
ESCUELA DE ELECTRÓNICA

RECTOR
ING. FEDERICO MIGUEL HUGUET

SECRETARIO GENERAL
LIC. MARIO RAFAEL OLMOS

DECANO FACULTAD DE INGENIERIA
ING. ERNESTO GODOFREDO GIRON

SEPTIEMBRE 2008
EL SALVADOR CENTROAMERICA

UNIVERSIDAD DON BOSCO
FACULTAD DE INGENIERÍA
ESCUELA DE ELECTRÓNICA

TRABAJO DE GRADUACIÓN
PARA OPTAR AL TITULO DE
INGENIERO EN TELECOMUNICACIONES

DESCRIPCIÓN, COMPROBACIÓN DEL FUNCIONAMIENTO Y DE LAS APLICACIONES DISPONIBLES DE DISPOSITIVOS UTM (UNIFIED THREAT MANAGEMENT).

ASESOR
ING. FRANCISCO ROBLES

LECTOR
ING. JUAN CARLOS CASTRO

SEPTIEMBRE 2008
EL SALVADOR CENTROAMERICA

AGRADECIMIENTOS

A Dios, que me ha permitido concluir esta etapa de mi vida y, por regalarme a mi familia y amigos, que me han brindado su apoyo, haciendo de una u otra forma más sencillo el camino recorrido, para alcanzar esta meta.

DEDICATORIA

A toda mi familia que con mucho sacrificio, esfuerzo, pero sobretodo con amor me han dejado la herencia más valiosa: la educación.

INDICE

I. INTRODUCCION ..... **- 1 -**

II. OBJETIVOS ..... **- 2 -**

2.1 Objetivo General: ..... **- 2 -**

2.2 Objetivos Específicos: ..... **- 2 -**

III. ALCANCES Y LIMITACIONES ..... **- 3 -**

3.1 Alcances: ..... **- 3 -**

3.2 Limitantes: ..... **- 3 -**

IV. MARCO TEORICO ..... **- 4 -**

Capitulo 1: Introducción ..... **- 5 -**

1.0 EVOLUCION DE LOS SISTEMAS DE SEGURIDAD ..... **- 6 -**

1.0.1 Firewall. ..... - 6 -

1.1 Firewall de Filtrado de Paquetes. ..... **- 7 -**

1.1.1 Descripción del filtrado de paquetes ..... - 7 -

1.1.2 Configuraciones de cadenas ..... - 9 -

1.1.3 Análisis de paquetes ..... - 12 -

1.1.4 Resumen. ..... - 14 -

1.2 Firewall de Filtro de Estado ..... **- 15 -**

1.2.1 Funcionamiento ..... - 15 -

1.2.2 Resumen. ..... - 17 -

1.3 Firewall de Capa de Aplicación. ..... **- 18 -**

1.3.1 Descripción ..... - 19 -

1.3.2 Funcionamiento ..... - 20 -

1.3.3 Resumen ..... - 21 -

1.4 Firewall de Inspección de Estado. ..... **- 22 -**

1.4.1 Descripción. ..... - 22 -

1.4.2 Análisis de paquetes. ..... - 24 -

1.4.3 Resumen. ..... - 25 -

1.5 Deep Packet Inspection. ..... **- 25 -**

1.5.1 Descripción ..... - 26 -

1.5.2 Tipos de análisis. ..... - 27 -

1.5.2.1 Análisis por puerto. ..... - 28 -

1.5.2.2 Similitud de cadenas ..... - 28 -

1.5.2.3 Análisis de propiedades numéricas ..... - 29 -

1.5.2.4 Análisis por comportamiento y de manera heurística. ..... - 29 -

1.6 Software Firewalls & Hardware Firewalls. ..... **- 31 -**

1.6.1 Firewalls por Software ..... - 31 -

1.6.2 Hardware ..... - 32 -

1.6.3 Proxy. ..... - 33 -

Capitulo 2: Introducción. ..... **- 35 -**

2.0 DESCRIPCION DE DISPOSITIVOS UTM ..... **- 36 -**

2.0.1 Firewall. ..... - 38 -

2.1 Filtrado de Contenido Web ..... **- 39 -**

2.2 Prevención de Intrusos. ..... **- 42 -**
2.2.1 Tipos de Ataques más Comunes ..... - 45 -
a) Sniffing ..... - 45 -
b) IP spoofing ..... - 45 -
c) DoS: Denial of Service ..... - 45 -
d) Net Flood ..... - 46 -
e) DDoS ..... - 46 -
f) Ping of Death ..... - 47 -
g) Troyanos ..... - 47 -
2.2.2 Técnicas usadas en IDS e IPS ..... - 48 -

2. 3 Redes privadas virtuales. ..... **- 50 -**
2.3.1 Características. ..... - 51 -
2.3.2 Tipos de VPN ..... - 52 -
2.3.2.1 VPN IPSec ..... - 53 -
2.3.2.1.1 Características de IPSec ..... - 54 -
2.3.2.2.2 Funcionamiento de IPSec ..... - 56 -
2.3.2.2.3 El protocolo IKE ..... - 57 -
2.3.2.2 VPN SSL ..... - 58 -
2.3.2.2.1 Características de SSL ..... - 59 -
2.3.2.2.2 Funcionamiento de SSL ..... - 60 -

2.4 Anti Spam. ..... **- 63 -**
2.4.1 Introducción. ..... - 63 -
2.4.2 Spam ..... - 64 -
a) Spam por mensajería instantánea: ..... - 64 -
b) Spam en grupos de noticias, blogs o foros: ..... - 64 -
c) Spam en telefonía móvil: ..... - 64 -
2.4.2.1 Métodos de Detección de Spam ..... - 67 -
a) Filtrado de Contenido ..... - 67 -
b) RBL (Real Time Black Holes) ..... - 67 -
c) Análisis Heurístico ..... - 68 -
d) Filtros Bayesianos ..... - 68 -
e) Checksums ..... - 69 -
f) SpamPost ..... - 70 -
g) Listas Grises ..... - 70 -

2.5 Antispyware. ..... **- 72 -**
2.5.1 Introducción. ..... - 72 -
2.5.2 Tipos de Spyware. ..... - 73 -

2.6 Antivirus. ..... **- 75 -**
2.6.1 Clasificación de los Virus. ..... - 75 -
2.6.1.1 Virus de Fichero. ..... - 76 -
2.6.1.2 Virus de Boot ..... - 77 -
2.6.1.3 Virus de Macro ..... - 78 -
2.6.1.4 Virus de enlace o de directorio ..... - 79 -
2.6.2 Técnicas de Infección. ..... - 80 -
2.6.3 Antivirus ..... - 82 -

2.7 IM & P2P ..... **- 84 -**
2.7.1 P2P ..... - 84 -
2.7.1.1 Configuraciones lógicas de redes P2P ..... - 85 -
2.7.1.2 Generaciones de P2P ..... - 86 -
2.7.2 IM ..... - 89 -
3.7.2.1 Funcionamiento IM ..... - 90 -
2.7.3 Métodos para identificar protocolos ..... - 93 -
2.7.3.1 Técnica heurística ..... - 93 -

2.7.3.2 Patrones ..... - 94 -
2.7.3.3 Firmas ..... - 95 -

2.8 Reportes. ..... **- 97 -**

2.9 Áreas no cubiertas ..... **- 99 -**

Capitulo 3: Introducción ..... **- 101 -**

3.0 UTILIDAD DE DISPOSITIVOS UTM ..... **- 102 -**

3.1 Controlar tráfico en la red ..... **- 102 -**
3.1.1 Técnicas usadas para filtrar contenido web ..... - 104 -

3.2 Regular acceso de los usuarios a Internet ..... **- 106 -**
3.2.1 Modalidades de configuración de usuarios ..... - 108 -

3.3 Sistemas de seguridad en la red ..... **- 109 -**
3.3.1 Identificación de tráfico (IDS) ..... - 110 -
3.3.2 IPS y Antivirus ..... - 111 -

3.4 Creación de VPN confiables ..... **- 114 -**
3.4.1 VPN SSL ..... - 115 -
3.4.2 VPN IPSec ..... - 116 -

3.5 Complementos Adicionales ..... **- 118 -**
3.5.1 Aplicaciones P2P/IM ..... - 118 -
3.5.2 Reportes. ..... - 120 -

Capitulo 4: Introducción ..... **- 122 -**

4.0 COMPARACIÓN ENTRE DISPOSITIVOS UTM. ..... **- 123 -**
4.0.1 Introducción. ..... - 123 -

4.1 Pruebas de equipos. ..... **- 124 -**
4.1.1 Pruebas a realizar. ..... - 124 -

4.2 Fortinet. ..... **- 125 -**
4.2.1 Aspectos generales. ..... - 125 -
4.2.2 Técnicas utilizadas. ..... - 126 -
4.2.3 Equipo Fortinet. ..... - 131 -
4.2.3.1 Elementos generales. ..... - 131 -
4.2.3.2 Descripción del menú principal y las sub categorías más importantes. ..... - 132 -
a) System ..... - 132 -
b) Router ..... - 133 -
c) Firewall ..... - 134 -
d) VPN ..... - 135 -
e) User ..... - 136 -
f) Antivirus ..... - 136 -
g) Intrusion Protection: ..... - 137 -
h) Web Filter ..... - 137 -
i) Antispam ..... - 138 -
j) IM, P2P & VoIP ..... - 138 -
k) Log & Report ..... - 138 -
4.2.3.3 Parámetros Básicos. ..... - 139 -
4.2.3.4 Configuración de VPN ..... - 143 -
a) VPN SSL ..... - 143 -
b) VPN IPSEC ..... - 146 -
4.2.3.5 Configuración de Perfiles ..... - 148 -
4.2.3.6 Filtrado de contenido web ..... - 151 -
4.2.3.6.1 Filtrado web estático ..... - 151 -

4.2.3.6.2 Filtrado web dinámico ..... - 154 -
4.2.3.7 IM&P2P ..... - 157 -
4.2.3.7.1 IM ..... - 157 -
4.2.3.7.2 P2P ..... - 160 -
4.2.3.8 IPS ..... - 161 -
4.2.3.9 Antivirus ..... - 163 -
4.2.3.10 AntiSpam ..... - 164 -
4.2.3.11 Reportes ..... - 166 -

4.3 SonicWALL ..... **- 170 -**
4.3.1 Aspectos generales ..... - 170 -
4.3.2 Técnicas utilizadas ..... - 172 -
4.3.3 Equipo SonicWALL ..... - 174 -
4.3.3.1 Elementos generales ..... - 174 -
4.3.3.2 Descripción del menú principal y las sub categorías más importantes ..... - 176 -
a) System. ..... - 176 -
b) Network ..... - 178 -
c) PC Card ..... - 179 -
d) Firewall ..... - 180 -
e) VPN ..... - 181 -
f) Users ..... - 181 -
g) Security Services ..... - 182 -
h) Log ..... - 184 -
i) Wizards ..... - 184 -
j) Help ..... - 185 -
4.3.3.3 Parámetros Básicos ..... - 185 -
4.3.3.4 Configuración de VPN ..... - 186 -
4.3.3.5 Configuración de perfiles. ..... - 189 -
4.3.3.6 Filtrado de contenido web ..... - 192 -
4.3.3.7 IM&P2P ..... - 194 -
4.3.3.8 IPS ..... - 196 -
4.3.3.9 Antivirus. ..... - 198 -
4.3.3.10 Anti-Spyware ..... - 200 -
4.3.3.11 Análisis de Correo ..... - 201 -
4.3.3.12 Reportes ..... - 202 -
4.3.3.13 Wizards ..... - 204 -

4.4 Conclusiones de las Pruebas realizadas. ..... **- 205 -**
4.4.1 Creación de perfiles. ..... - 207 -
4.4.2 Configuración de VPN ..... - 208 -
4.4.3 Web Filtering ..... - 209 -
4.4.4 P2P/IM ..... - 210 -
4.4.5 IPS ..... - 211 -
4.4.6 Antivirus, Antispyware y Antispam. ..... - 212 -
4.4.7 Reportes ..... - 213 -

V. CONCLUSIONES. ..... **- 215 -**

VI. RECOMENDACIONES. ..... **- 217 -**

VII. BIBLIOGRAFIA Y FUENTES DE CONSULTA. ..... **- 218 -**

VIII. GLOSARIO. ..... **- 222 -**

IX. ANEXOS. ..... **- 230 -**

Anexo 1: Hojas Técnicas de los Equipos Utilizados. ..... **- 230 -**

I. INTRODUCCION

En el siguiente trabajo se presenta información relacionada a los dispositivos UTM (Unified Threaten Management), se describe de forma general la diversidad de áreas que estos dispositivos enmarcan en su plan de acción y como estas medidas pueden beneficiar en la administración y correcto desempeño de una red informática.

Se han separado en cinco capítulos diversos enfoques del accionar de estos dispositivos, primeramente se hace una breve introducción a los conceptos de redes de comunicaciones describiendo los puntos que se utilizaran posteriormente en el mismo documento. Luego se realiza una breve descripción de las evoluciones que los antecesores de estos equipos han tenido a través de la historia, enfocando sus principales características hasta llegar a la técnica usada por los equipos estudiados.

La parte central del documento está conformado por la descripción de la estructura aplicativa de un dispositivo UTM, enfocando las áreas cubiertas por cada modulo y las técnicas usadas en cada una de ellas. Posteriormente se presenta la descripción del uso de un dispositivo UTM y de cómo estos pueden beneficiar en la administración del eficiente desempeño de red. Finalmente se hace un estudio de comprobación de aplicaciones entre dos de estos dispositivos basándose en las necesidades básicas que estos según sus características deberían de cumplir.

El documento fue elaborado sin apegarse a una marca o fabricante especifico, sino más bien tratando de enfocar de manera general a un buen numero de los dispositivos utilizados en el mercado. Para la conformación de este, se utilizaron en su gran mayoría fuentes bibliográficas de Internet debido a que la información existente en este ámbito es mucho mayor que la que se encuentra en formato bibliográfico tradicional y se tiene la opción de contar con datos más actuales.

II. OBJETIVOS

2.1 Objetivo General:

- Dar a conocer de manera general la evolución, y de manera más detallada el funcionamiento y las aplicaciones de los dispositivos UTM

2.2 Objetivos Específicos:

- Hacer una breve reseña de la evolución de los dispositivos de seguridad informática que han existido a lo largo de la historia hasta llegar a los UTM.

- Presentar los dispositivos UTM como más que un simple firewall, el cual puede solventar muchos de los problemas comunes de seguridad o de desempeño de red que se presentan frecuentemente a los administradores de red.

- Hacer una comparación entre un par de dispositivos existentes en el mercado, para presentar sus fortalezas y debilidades.

III. ALCANCES Y LIMITACIONES

3.1 Alcances:

- Presentar una breve descripción de la evolución de los sistemas de seguridad a través de la historia hasta llegar a nuestros días.

- Dar a conocer los dispositivos UTM, además de describir sus características, funcionalidades y limitantes, sin enfocarse en un fabricante en especial sino realizarlo de manera general.

- Comprobar de manera general su funcionalidad y limitantes con dos equipos.

3.2 Limitantes:

- Multiplicidad de información dependiendo del fabricante y modelo de equipo consultado.

- Restringido acceso a los dispositivos para poder comprobar la funcionalidad de estos dispositivos.

IV. MARCO TEORICO

El marco teórico se dividirá en 5 capítulos, los que se presentan a continuación:

- Capitulo 1:
  Evolución de Sistemas de Seguridad Informática.

- Capitulo 2:
  Descripción de Dispositivos UTM.

- Capitulo 3:
  Utilidad/Aplicaciones de Dispositivos UTM.

- Capitulo 4:
  Comparación entre Dispositivos.

Capitulo 1: Introducción

En el siguiente capítulo se muestran las técnicas usadas para la seguridad informática, se presentan las características de los métodos usados a través del tiempo moderno, en donde se inicia con la presentación del firewall por filtrado de paquetes, hasta llegar a la técnica Deep Packet Inspection la cual es usada en la actualidad por los dispositivos UTM, se describe cada uno de los cinco modelos usados presentando sus ventajas y deficiencias.

Esto ya que es necesario dar a conocer la evolución de los sistemas y la razón por la cual han evolucionado de esa manera, ya que en la actualidad todas las técnicas siguen vigentes y cada una ha servido como base para la siguiente.

Finalmente en el capítulo se presentan tres diversas alternativas que pueden proporcionar seguridad en la red informática, entre ellas están los firewalls por software, los firewall por hardware y los proxies.

1.0 EVOLUCION DE LOS SISTEMAS DE SEGURIDAD

Antes de iniciar con la definición del término UTM, se debe de hacer una breve retrospectiva e indicar de donde surgió la iniciativa de estos dispositivos como tales; para lo cual se debe de mencionar el termino firewall, el cual es considerado el antecesor directo de estos dispositivos

1.0.1 Firewall.

Un firewall se define como un sistema cuya finalidad es hacer cumplir una política de control de acceso entre dos redes interconectadas, generalmente es colocado para proteger a una red confiable (red interna) de una red no confiable (generalmente Internet), delimitando y controlando el tráfico entre ellas. Esto se puede observar gráficamente en la figura 1.1.

La historia de los firewalls, comenzó aproximadamente en los finales de los ochentas, para ese entonces el Internet era una herramienta relativamente nueva, además estaba reservada para pocos privilegiados, de hecho fue en las oficinas de la NASA en donde se pensó en dispositivos de seguridad, al crear un virus y propagarlo por la red por medio de un correo electrónico, sin haber sido un código malicioso se pudieron comprobar las vulnerabilidades de las computadoras de aquel entonces.

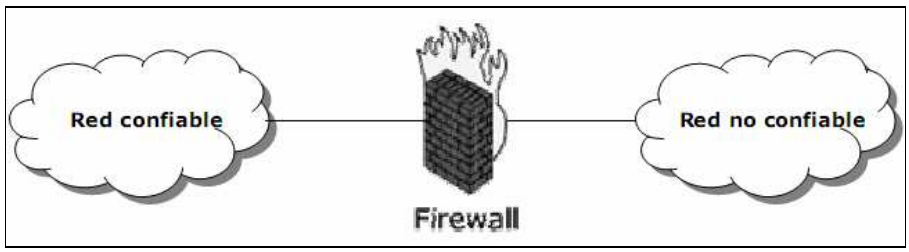


Figura 1.1 Ubicación típica de los Firewall en las redes.

Los firewalls a través de la historia han ido evolucionando tanto en sus tecnologías de análisis y clasificación de tráfico como en su presentación ofrecida al público por parte de los fabricantes. A continuación se presenta una breve descripción de los tipos de firewalls que a lo largo de la historia se han tenido, de hecho se presentan los más significativos ya

que pudieran existir muchas clasificaciones o puntos de vista de la evolución, sin embargo se han descrito los más significativos hasta llegar a los que dieron origen a los dispositivos UTM.

1.1 Firewall de Filtrado de Paquetes.

Los firewalls tienen su inicio en Noviembre de 1988, a partir del suceso antes mencionado en la NASA, se concibieron con ciertas definiciones específicas como: “es un punto entre dos o más redes por el cual todo el tráfico que se intercomunica entre ellas tiene que pasar” y “todo el tráfico monitoreado es controlado y registrado por este dispositivo”. Los primeros firewalls que aparecieron eran Routers usados para separar las redes en pequeñas LAN’s, sobretodo dividían los segmentos problemáticos para que estos no afectaran el desempeño de la red completa.

La tecnología de filtrado de paquetes fue desarrollada por ingenieros de la DEC (Digital Equipment Corporation), empresa pionera en el ámbito de la computación en Estados Unidos. Esta funciona entre la capa de transporte y la capa de red del protocolo TCP/IP y como su nombre lo indica se analizan paquetes y se toman decisiones en base al contenido de estos.

1.1.1 Descripción del filtrado de paquetes

El filtrado de paquetes se realiza analizando los encabezados de los paquetes IP que llegan al equipo donde se encuentra instalado el firewall, estos encabezados son comparados con listas que contienen permisiones o denegaciones del trafico entrante a la red según sea la estructura o el origen del tráfico basándose únicamente en su encabezado, luego en base al resultado obtenido de estas comparaciones se toman decisiones de enrutamiento, es decir se decide si estos paquetes son filtrados accesando así a la red interna o son descartados por el firewall.

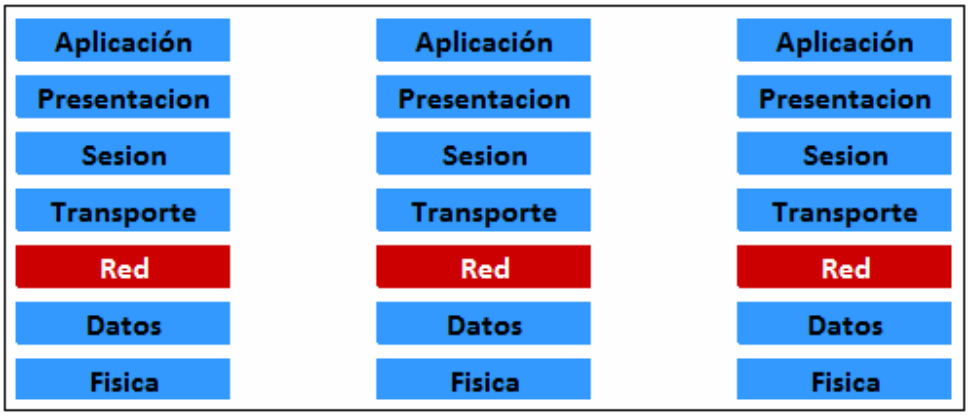


Figura 1.2 Ilustración de la operación en las capas del modelo OSI del filtrado de paquetes

Estas listas que sirven para las comparaciones de los paquetes, a su vez contienen en su interior reglas de aceptaciones o denegaciones, estas reglas definen explícitamente a los paquetes que se aceptaran o se denegaran por el firewall, usando los encabezados de cada paquete para decidir si se aceptan los paquetes, se rechazan o se deniegan. La información que se "evalúa" en los encabezados de cada paquete puede ser: información de IP origen o destino de la capa de red, los puertos de servicio TCP o UDP de la capa de transporte , los indicadores de conexión TCP, los tipos de mensaje ICMP del nivel de red y si el paquete es entrante o saliente. Lo anterior se muestra en la figura 1.3.

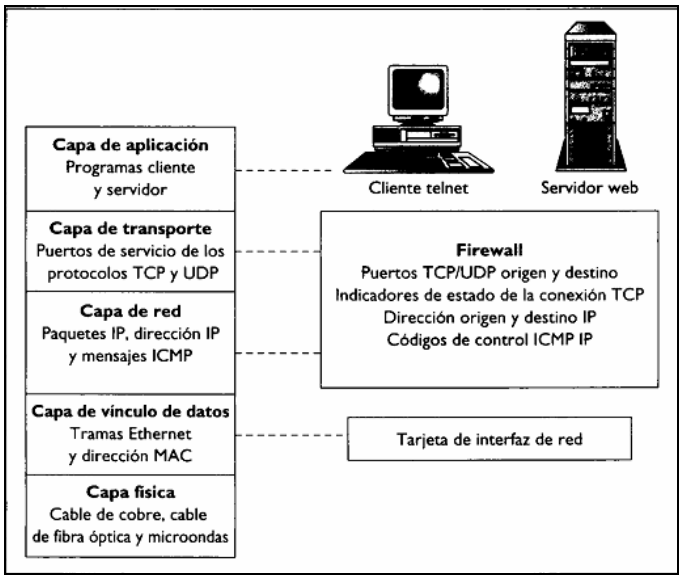


Figura 1.3 Ilustración de la operatividad del filtrado de paquetes

Las listas de aceptaciones y denegaciones antes mencionadas se les conoce también como cadenas, estas funcionan realizando comparaciones entre cada paquete IP que se recibe y cada una de las reglas en la lista, se compara una a una cada regla hasta que se encuentra una coincidencia del paquete entrante con alguna de estas o hasta que se termina la lista, esto se ilustra en la figura 1.4.

Como se observa el filtrado de paquetes es un método exhaustivo de seguridad más no es infalible, esto debido a que es un nivel de seguridad relativamente bajo debido a que no todas las aplicaciones se mueven entre las capas que este método examina, por ejemplo se utiliza como parámetro la verificación de identidad del emisor de paquetes siendo esta información fácil de modificar.

1.1.2 Configuraciones de cadenas

En lo que respecta a las reglas de cadenas existentes, se puede hablar de dos perspectivas básicas para las reglas de un firewall:

- Denegar todo por defecto y permitir acceso a paquetes seleccionados explícitamente.
- Aceptar todo por defecto y denegar acceso a paquetes seleccionados explícitamente.

De las dos perspectivas antes mencionadas, se recomienda realizar la primera, aunque sea la más complicada de configurar, ya que de esta forma únicamente se permite el acceso a las aplicaciones conocidas y deseadas. Si se realiza la alternativa de aceptar todo por defecto, solo se negaría el acceso a las amenazas conocidas, generando huecos de seguridad para el acceso a la red interna, esto se ilustra en la figura 1.5.

Cabe mencionar que por el tipo de análisis que se realiza con esta técnica, se requieren de extensas cadenas para lograr identificar un mayor número de aplicaciones con veracidad, esto es posible siempre y cuando se conozcan a cabalidad las aplicaciones implicadas en el tráfico, para así lograr que el filtrado sea efectivo y por tanto las herramientas de seguridad de la red se incrementen. Por otro lado existe el inconveniente que las aplicaciones nuevas serán denegadas si no se actualizan las cadenas indicando lo contrario.

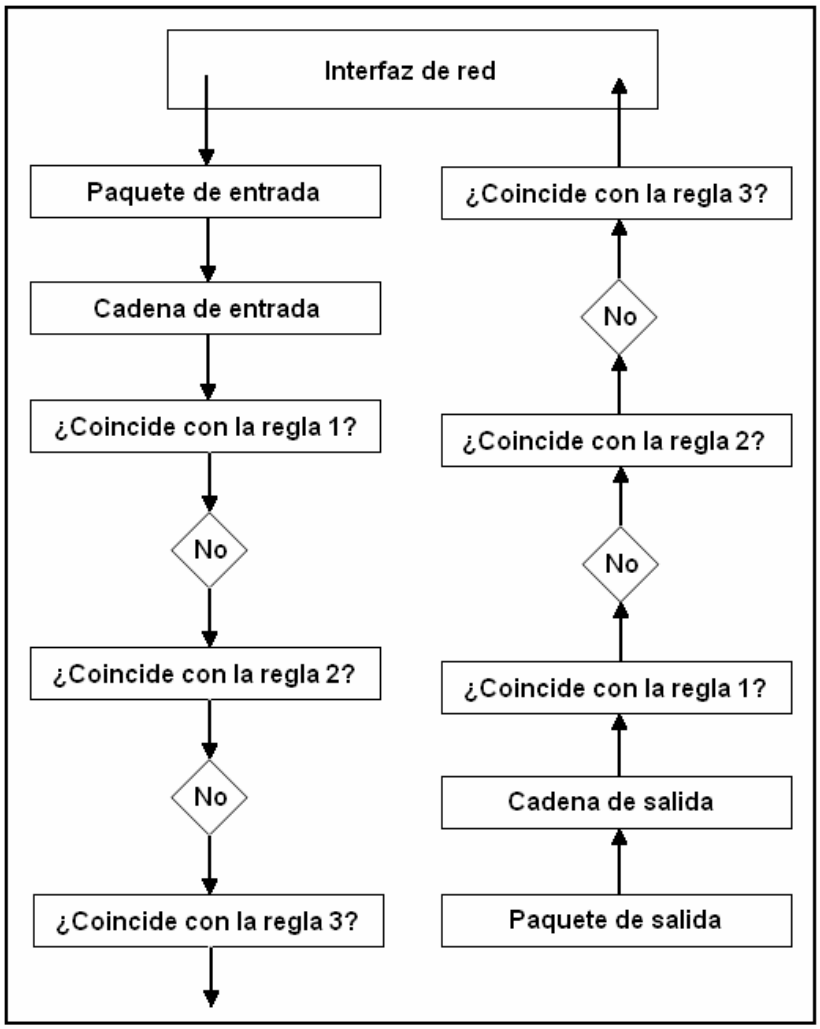


Figura 1.4 Algoritmo las Cadenas

Un punto importante a mencionar es la diferencia entre la denegación y el rechazo de paquetes; a pesar que en ambos métodos se desechan los paquetes al no concordar con la lista respectiva. Esta discrepancia se presenta en la respuesta obtenida después de desechar los paquetes, cuando se rechaza un paquete este se descarta y se devuelve un mensaje de error ICMP al remitente, pero cuando se deniega un paquete simplemente se descarta el paquete sin notificar al emisor, el flujograma de esto se presenta en la figura 1.6.

Esta última es la opción más recomendada, primero debido a que si se envía una respuesta de error se duplica el tráfico de la red, segundo porque cualquier paquete al que se responda se puede usar en un ataque por denegación de servicio o puede contener información útil para cualquier ataque posterior.

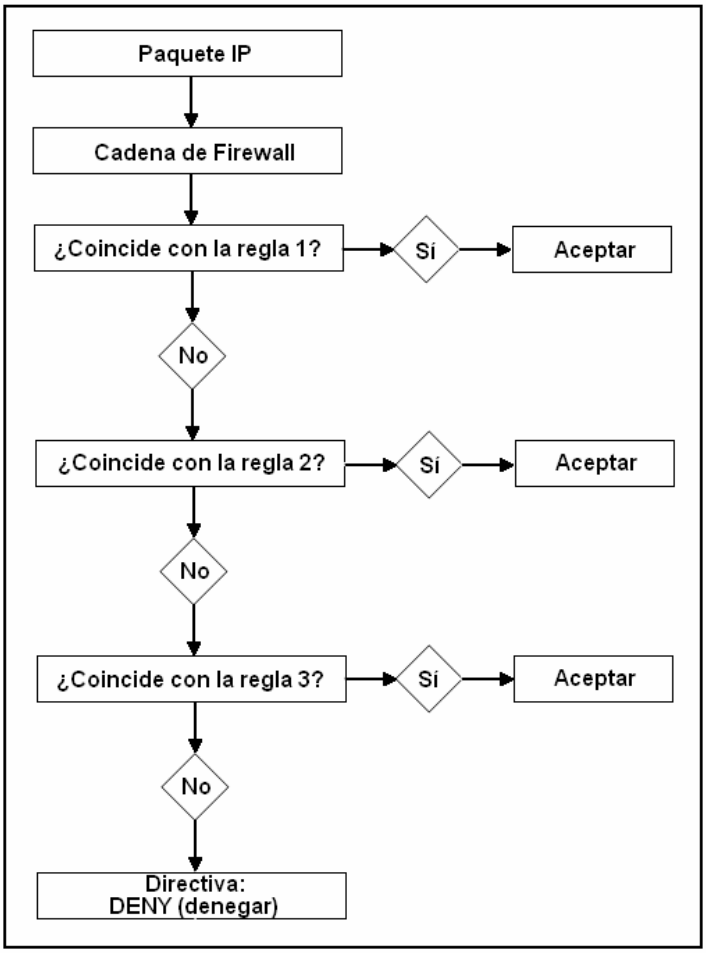


Figura 1.5. Flujograma de lista con perspectiva de denegar todo

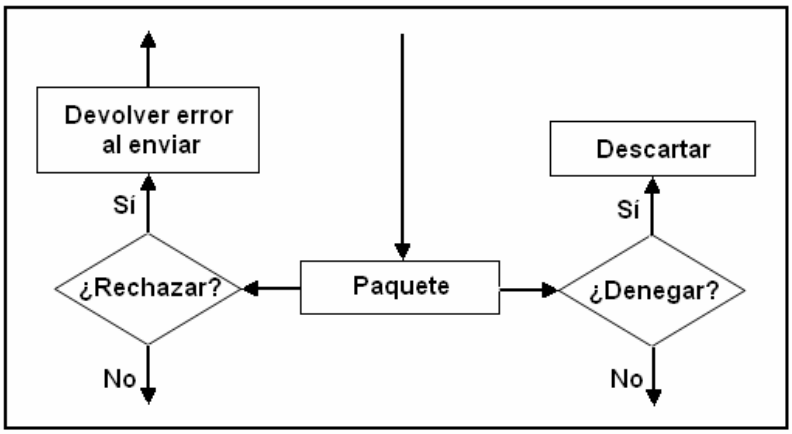


Figura 1.6 Flujograma de Rechazar o Denegar paquetes

1.1.3 Análisis de paquetes

En lo que respecta al análisis de los paquetes de entrada, que generalmente es la que siempre se verifica y la que más importancia tiene; se puede filtrar basándose en la dirección origen, la dirección destino, el puerto origen, el puerto destino y el indicador de estado TCP, para el caso de aplicaciones UDP no se recomienda utilizar este tipo de filtrado ya que este trafico UDP suele seleccionar puertos aleatorios (superiores a 1023) para su comunicación lo que dejaría más desprotegida la seguridad en la red.

Como ya se mencionó anteriormente, el único medio de identificar el remitente del paquete IP es la dirección origen del encabezado de paquete, por lo tanto siendo bastante susceptible al spoofing o cambio de dirección origen, donde el remitente coloca una dirección incorrecta ya sea esta inexistente u otra dirección en lugar de la suya en el campo origen, esto con el fin de usurpar información o monitorear el trafico existente entre dos puntos en la red. En la figura 1.7 se presenta la ilustración de los campos a evaluar en un paquete IP.

Para contrarrestar en parte esta posible vulnerabilidad de estos sistemas, se recomienda tomar en cuenta en las configuraciones de las reglas los siguientes puntos:

- Bloqueo de direcciones privadas provenientes de Internet al firewall, tanto clase A, clase B, clase C, clase D y clase E, permitiendo así únicamente el acceso de direcciones públicas desde Internet hacia el Firewall.
- Bloqueo de direcciones de interfaz de bucle invertido, el trafico de bucle invertido o pruebas de loopback esta enrutado hacia el mismo sistema que lo generó, es decir siempre apunta al host que genera el trafico hacia la red, son consideradas pruebas de localhost e incluyen rangos desde la IP 127.0.0.0 hasta la 127.255.255.255, por lo consiguiente se le debe restringir el acceso a este rango desde Internet hacia el Firewall.
- Bloqueo de la dirección de difusión mal formada, esta es la dirección 0.0.0.0 usada por los servidores de DHCP ya que ellos enviaran con esta IP a todos los clientes la información de las direcciones IP asignadas, es decir los clientes verán los paquetes entrantes a ellos provenientes de esta dirección. Por lo consiguiente no debería de existir una IP como esta a la entrada de una red externa de un firewall.

- Bloqueo o restricción de sesiones Telnet al firewall o equipos en la red interna, delimitando o especificando únicamente las IP de las cuales será posible acceder desde fuera de la red.

Otra recomendación importante para contrarrestar la vulnerabilidad de seguridad, es el bloqueo de puertos lógicos, estos por defecto si se realizan peticiones desde la red interna hacia Internet deben de ser con puertos menores a 1024 y se recibirán peticiones con números de puertos entre 1024 y 65535. Como se observa es bastante el rango que queda sin cubrir y a esto hay que agregarle que algunas aplicaciones (como el IM y el P2P) pueden intercambiar de puertos de comunicación al encontrarse bloqueados los que ellos usan originalmente.

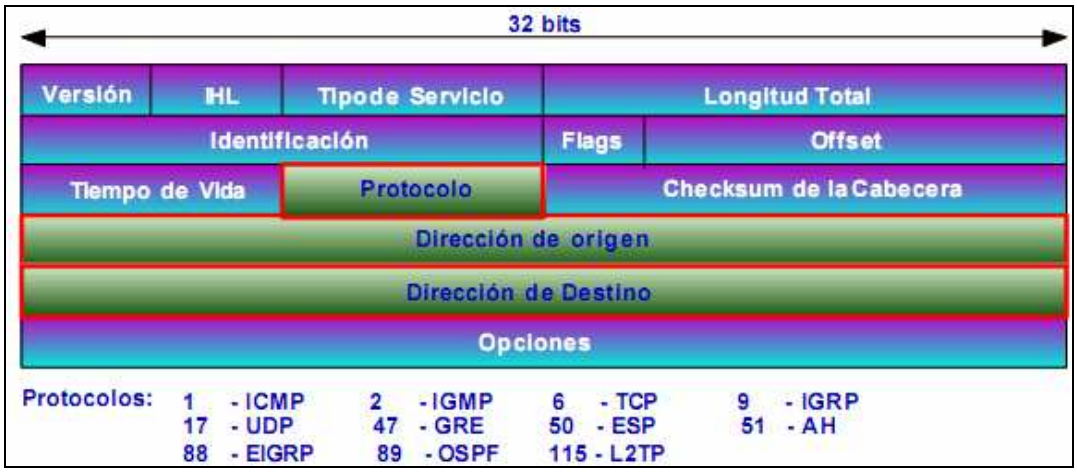


Figura 1.7. Cabecera de un paquete IPV4. Muestra los campos que habitualmente inspeccionan estos firewall y los Protocolos mayormente usados.

En cuanto a las reglas de estado de conexión TCP entrante, hay que tener en cuenta que los estados difieren entre cliente y servidor debido al saludo de tres vías que se realiza durante el establecimiento de la conexión. Los paquetes TCP entrantes procedentes del cliente remoto tendrán el indicador SYN activado en el primer paquete recibido como parte del saludo antes mencionado. La primera petición de conexión tendrá el indicador SYN activado, pero no el ACK, por lo que todos los paquetes entrantes después de la primera petición de conexión tendrán solo el indicador ACK activado. Las reglas del firewall del servidor local permitirán paquetes entrantes, sin tener en cuenta el estado de los indicadores SYN y ACK.

Los paquetes entrantes procedentes de servidores remotos siempre serán respuestas a la petición de conexión inicial que comienza en el programa cliente local. Cada paquete recibido desde un servidor remoto tendrá el indicador ACK activado; las reglas del firewall cliente local solicitaran que todos los paquetes entrantes procedentes de servidores remotos tengan el indicador ACK activado. Los servidores legítimos no intentaran iniciar conexiones a programas cliente.

1.1.4 Resumen.

Principales ventajas:

1. Bajo costo de implementación.
2. Puede ser implementando con rapidez en lugares donde no es recomendable tener una instalación de firewall completa.
3. Fácil configuracion y mantenimiento.
4. Aplicación detallada de seguridad a bajo nivel.
5. Elemento transparente para el usuario de la red interna.

Las principales desventajas que esta técnica ofrece tenemos:

1. No protege las capas superiores a nivel OSI.
2. Las necesidades aplicativas son difíciles de traducir como filtros de protocolos y puertos.
3. No son capaces de esconder la topología de redes privadas, por lo que exponen la red al mundo exterior.
4. Sus capacidades de auditoria suelen ser limitadas, al igual que su capacidad de registro de actividades.
5. No soportan políticas de seguridad complejas como autentificación de usuarios y control de accesos con horarios prefijados.
6. Intercambian la totalidad de paquetes entre la red externa e interna.

1.2 Firewall de Filtro de Estado.

Entre los años de 1988 a 1991 científicos de los laboratorios Bell AT&T, utilizaron una segunda técnica para crear firewalls, a esta se le llamo firewalls de nivel de circuitos. Estos corregían algunos puntos de sus antecesores, ya que si le importaba la ubicación de los paquetes en la trama y se tenían partes confiables en la comunicación consideradas como tramas conocidas.

El nombre de filtros de estado proviene de la capacidad que estos firewalls tenían en identificar si un paquete era inicio, final o simplemente parte de una trama, el cual es un punto importante a la hora de activar reglas especificas en los análisis del tráfico. Este tipo de filtrado es capaz de proteger los ataques de denegación de servicio.

Aunque aun se realizaban las configuraciones desde routers propiamente dichos, con reglas un tanto sencillas como: “de la Red A nadie puede acceder a la Red B” o “la Red A solo puede ser vista por algunos elementos conocidos de la Red B”. Estos firewalls eran efectivos, pero también limitados por la misma sencillez de las reglas que se aplicaban contrastadas con los recursos informáticos entonces existentes.

1.2.1 Funcionamiento

Llamados firewalls de segunda generación o de nivel de circuitos, son firewalls de filtrado de paquetes en los que, se verifica a la hora de aceptar o rechazar un paquete el hecho de que este sea una petición de nueva conexión o pertenezca a un circuito virtual (o sesión) ya establecido entre un host externo y otro interno.

Cuando una aplicación crea una sesión TCP con un host remoto, se establece un puerto en el sistema de origen de la conexión con objeto de recibir allí los datos provenientes del sistema remoto. De acuerdo a las especificaciones de TCP, este puerto del host cliente estará comprendido entre el 1023 y el 16.384. En el sistema remoto se establecerá, asimismo, un puerto que será siempre menor al 1024.

Los firewalls por filtrado de paquetes deben de permitir tráfico entrante en todos los puertos superiores (1023 hasta 16.384) para permitir los datos de retorno de las conexiones salientes. Esto crea un gran riesgo de intrusiones. Los firewalls con inspección de estado resuelven eficazmente este problema construyendo una tabla con información

correspondiente a todas las sesiones TCP abiertas y los puertos que utilizan para recibir los datos y no permitiendo el tráfico entrante a ningún paquete que no corresponda con ninguna de estas sesiones y puertos.

Para hacer esto, el firewall de este tipo examinan rigurosamente el establecimiento de cada conexión (en la capa 4 del modelo OSI) para asegurarse de que esta es legítima y está permitida. Los paquetes no son remitidos a su destino hasta que el establecimiento de la conexión ha sido correctamente completado y verificado.

El equipo mantiene una tabla de conexiones válidas y deja pasar los paquetes que contienen información correspondiente a una entrada válida en dicha tabla de circuitos virtuales. Una vez que la conexión finaliza la entrada en la tabla es eliminada y el circuito virtual entre los dos hosts es cerrado.

Las tablas de estado de circuitos virtuales suelen contener la siguiente información:

- Un identificador de sesión único asignado por el firewall a cada conexión establecida.
- El estado de la conexión: negociándose, establecida o cerrándose. (capa 4)
- El número de secuencia del último paquete (capa 4).
- La dirección IP origen de los datos (capa 3).
- La dirección IP destino de los datos (capa 3).
- La interfase física de red, si procede, a través de la que los paquetes llegan (capa 1).
- La interfase física de red, si procede, a través de la que los paquetes salen (capa 1).

Una visión grafica de dichos elementos se muestra en la figura 1.8.

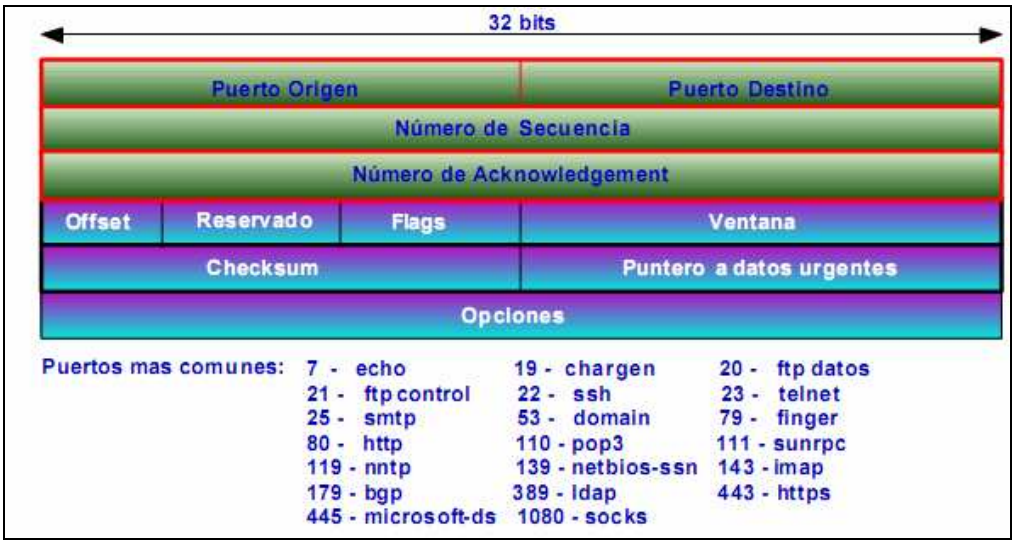


Figura 1.8. Cabecera TCP. Muestra los campos que verifica este tipo de firewall.

Usando esta información y con un ligero escrutinio de las cabeceras de los paquetes, el firewall es capaz de determinar cuando un paquete es válido y cuando no lo es. Una vez que la conexión es establecida, el resto de los paquetes asociados con ella son enrutados sin más comprobaciones. Esto los haría, tremendamente vulnerables a ciertos tipos de ataques, pero muy pocos firewalls de este tipo son tan rudimentarios ya que además realizan otro tipo de verificaciones para, por ejemplo, asegurarnos que no ha habido suplantamiento de identidad (spoofing), que no existen paquetes malformados, etc. También son comunes en ellos la implantación de sistemas de translación de direcciones, NAT, que ocultan eficazmente el interior de nuestra red a intrusos externos.

1.2.2 Resumen.

Ventajas

1. Velocidad de filtrado.
2 Protección de direcciones internas (NAT).
3 Principios bien fundamentados en su esquema de seguridad.

Desventajas:

1. Evaluación únicamente del protocolo TCP.
2. Seguridad de bajo nivel al chequear únicamente capa 3 y 4.

1.3 Firewall de Capa de Aplicación.

También conocida como generación de proxies, como dato curioso aquí se dio origen al primer equipo comercial de seguridad, el cual fue vendido en 1991 por la compañía DEC, a este se le conocía como DEC SEAL (Secure External Access Link), este estaba compuesto por un sistema externo llamado Gatekeeper, un sistema al cual se tenia acceso a Internet llamado Gate y en la parte de la LAN un MailHub. En la figura 1.9 se muestra el diagrama del DEC SEAL y una breve descripción de dichos elementos:

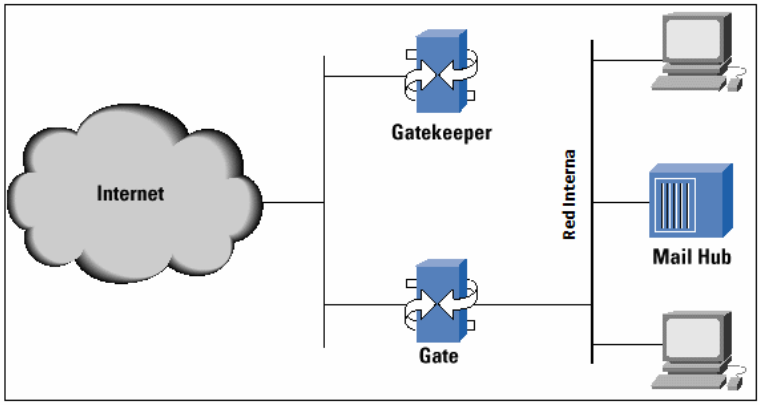


Figura 1.9 Diagrama del Firewall DEC SEAL

- ✓ *Gatekeeper*: server Proxy de aplicación para usuarios que tenían permitido el acceso a Internet, además de poder ser usado como un FTP o DNS anónimo.
- ✓ *Gate:* un router encargado de filtrar los paquetes y limitar el tráfico entre la red interna y la red externa. Este router era configurado para que todo el tráfico que entrara o saliera de la red interna se dirigiera al Gatekeeper.
- ✓ *Mailgate*: el server de mail's / router de mail's interno, esta maquina no era accesible desde fuera de la red interna. Si se enviara un mail desde fuera hacia la red interna, este tendría que ser entregado al Gatekeeper para luego enviarlo al Mailgate.

Esta tecnología presenta cambios significativos a sus antecesores, es capaz de analizar todas las capas superiores del modelo TCP/IP, de hecho su análisis se da en la capa de aplicación y es capaz de identificar no solo el puerto o la sesión, sino el protocolo que se utiliza, es decir identifica entre las diferentes aplicaciones que se intentan comunicar con la red interna, permitiendo las restricciones o accesos a partir del análisis en la capa de aplicación. Este firewall se instala en una maquina intermedia, es decir que separa la red interna de la externa, la cual recibe el nombre de pasarela de aplicación. El diagrama del

funcionamiento en las capas del modelo OSI de este tipo de firewalls se observa en la figura 1.10.

1.3.1 Descripción

La gran virtud de este tipo de dispositivos es la capacidad de diferenciar las aplicaciones y protocolos como por ejemplo FTP, DNS o HTTP, esto se realiza mediante una traducción en la aplicación ya que esta tecnología no utiliza el filtrado de paquetes IP. Además es capaz de detectar si una aplicación desconocida intenta comunicarse con puertos normalmente no utilizados para la comunicación.

Esta tecnología opera "enmascarando la identidad" de las maquinas de la red interna cuando se quiere acceder a una red externa, es decir un firewall Proxy opera sustituyendo la dirección origen del cliente por su dirección propia ante el servidor externo y cambiando la dirección del servidor externo por su dirección propia ante el cliente interno. Por lo anterior se dice que los servidores proxies garantizan la integridad de los datos, es decir que únicamente los datos que cumplan con los requisitos definidos en el Proxy tendrán libre acceso hacia la LAN y viceversa.

Los servicios o agentes típicos con que cuentan este tipo de dispositivos son: DNS, Finger, FTP, HTTP, HTTPS, LDAP, NMTP, SMTP y Telnet. Algunos fabricantes proporcionan agentes genéricos que, en teoría, son capaces de inspeccionar cualquier protocolo de la red, es decir se instala en el equipo que sustenta al firewall, un código de propósito especial (servicio Proxy) para cada aplicación deseada, si este código no ha sido instalado en dicho equipo el servicio no es soportado por el equipo rechazando dicho trafico.

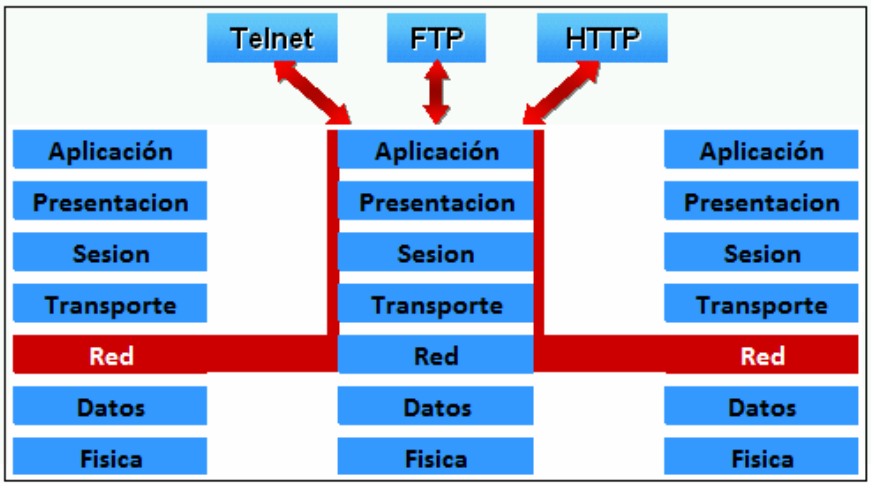


Figura 1.10 Ilustración de la operación en las capas del modelo OSI de los proxies

1.3.2 Funcionamiento

La traducciones que realizan estos equipos se generan mediante códigos de programas comúnmente llamados firmas, las cuales son capaces de identificar mediante patrones de trafico el tipo de aplicación que se esta intentando comunicar, esto ya sea de la red interna a la red externa o viceversa. Sin embargo, esto por tratarse de líneas de código ejecutables reduce grandemente la capacidad de rendimiento de la red.

Un servicio notable que prestan estos firewalls Proxy, es el concepto de caché que no es más que un pequeño historial de las paginas recién visitadas en la red, facilitando así una velocidad mayor en el acceso a dichas aplicaciones ya que al solicitar una pagina recién cargada, no hay necesidad de volver a hacer la petición a servidores externos, sino que se hace hacia el mismo firewall, optimizando así el ancho de banda ya que se realizan las solicitudes a servidores externos de páginas que no han sido visitadas recientemente.

Los agentes o servicios Proxy están formados por dos componentes: un servidor y un cliente. Ambos suelen implementarse como dos procesos diferentes lanzados por un único ejecutable. De esta forma estamos creando un aislamiento absoluto impidiendo una comunicación directa entre la red interna y la externa. En el diálogo entre cliente y servidor Proxy se evalúan las peticiones de los clientes de la red interna y se decide aceptarlas o rechazarlas en base a un conjunto de reglas, examinando exhaustivamente que los paquetes de datos sean en todo momento correctos. En la figura 1.11 se observa más detalladamente la segmentación y funcionamiento de un Proxy

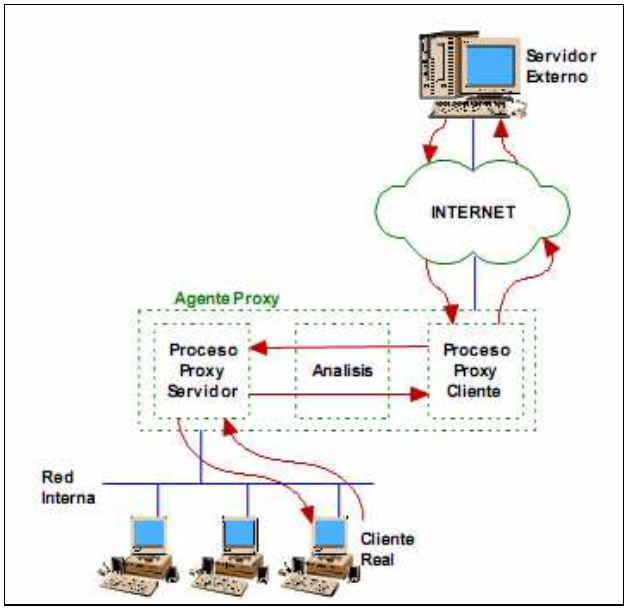


Figura 1.11 Segmentación de un firewall Proxy

El funcionamiento de estos firewalls puede darse de tres maneras posibles: modelo de seguridad positiva, modelo de seguridad negativa y combinación de ambos.

- ✓ El modelo de seguridad positiva consiste en identificar los patrones de tráfico legítimo y descartar todo aquel que no responda a dichos patrones.
- ✓ En el modelo de seguridad negativa se bloquea el tráfico reconocido como un intento de intrusión y se permite el resto.
- ✓ La combinación de ambos permite disponer del máximo grado de protección, flexibilizando las limitaciones de cada una de los modelos antes mencionados; de hecho es posible disponer de protección a lo desconocido sin la necesidad de un proceso de depuración ya que una vez que el firewall reconoce las aplicaciones que se desean proteger automáticamente se tiene el bloqueo contra las aplicaciones no conocidas o contra aplicaciones bien definidas por el administrador aumentando así el rendimiento del equipo ya que no se procesan completamente las aplicaciones comúnmente solicitadas.

1.3.3 Resumen

Ventajas:

1. Permiten protección de identidad.
2. Son capaces de soportar autenticación de usuarios para acceder a su configuración.
3. Capaces de guardar historial de sitios visitados y usuarios de la red.
4. Seguridad de alto nivel al cubrir la capa de aplicación.
5. Las reglas de acceso de trafico son mucho más sencillas de configurar que las que se tendrían que agregar para un filtra paquetes.

Desventajas:

1. Son los firewalls más lentos ya que dependen de programas para identificar el tráfico circulante.
2. Requieren de un administrador más especializado para la configuración de las políticas e identificación de las firmas.
3. Requieren actualización de las nuevas amenazas o aplicaciones implementadas para categorizar el tráfico de la red de la mejor manera.
4. Imposibilidad de inspeccionar protocolos comunes como UDP o RCP.

1.4 Firewall de Inspección de Estado.

En 1994 Check Point desarrollo el dispositivo Firewall-1, introduciendo para los usuarios el concepto de “interfaz amigable” en el mundo de la seguridad de redes, además de utilizar una técnica llamada inspección de estado, la cual consiste en filtrar paquetes y examinarlos con las capas superiores. Luego se introdujo el X11, el cual ya contaba con iconos y uso del mouse, facilitando de gran manera la configuración de estos equipos.

Esta versión del Firewall-1 aun sirve como base para los productos de Check Point, de hecho es una de las pocas tecnologías que sigue perteneciendo a la sociedad que la originó y desarrolló. Además, esta tecnología ha estado ligada a la creación de VPN desde un inicio. Los firewalls que utilizan la tecnología de Stateful Inspection también son llamados firewalls híbridos o firewalls de tercera generación, estos equipos utilizan el encolamiento de paquetes para luego analizarlos en todas las capas posibles del sistema OSI.

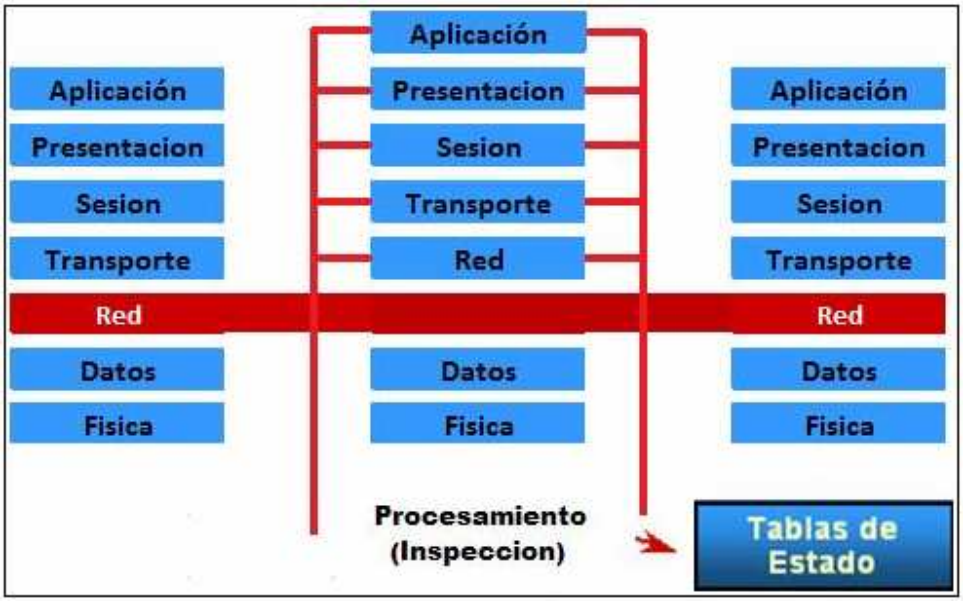


Figura 1.12 *Ilustración de la operación en las capas del modelo OSI para los firewalls de inspección de estado*

1.4.1 Descripción.

Esta tecnología utiliza conceptos del filtrado de paquetes y de los firewalls de aplicaciones, se interceptan los paquetes en la capa de red para obtener un mejor rendimiento similar al usado en el filtrado de paquetes, pero luego de ser interceptados se comparan con las capas

restantes para determinar si son paquetes de aplicaciones conocidas o permitidas. Permitiendo generar las restricciones o permisiones en cualquiera de las capas del modelo OSI a las que se tenga acceso en el análisis, esto se observa gráficamente en la figura 1.12.

Lo antes mencionado genera altos niveles de protección en la red ya que introducen niveles de seguridad en la comunicación y se tiene la ventaja de generar historial de la información circulante en la red y actualizaciones de la misma, proporcionando así historial con el cual se puede comparar en posteriores sesiones como podrían ser aplicaciones en UDP o RPC.

La verificación se realiza en base a factores como los tradicionales números de puertos, las direcciones IP involucradas, y quizás lo que lo hace diferente y sobresaliente el número de secuencia de tramas, este último se utiliza la información del inicio y el fin de trama para saber si cada trama contiene algún paquete alterado dentro de si y este pueda atravesar el firewall y llegar a la red interna, en la figura 1.13 se puede observar el análisis que se realiza en un paquete usando la técnica de inspección de estado. El punto clave para analizar cada trama es cuando se configura la conexión, es decir cuando se ingresa una nueva trama para el análisis respectivo, luego de haber determinado el inicio y el final de la trama se crea un circuito virtual entre los host involucrados, una vez teniendo estos circuitos lógicos el análisis de los paquetes intermedios se realiza sin mayores complicaciones.

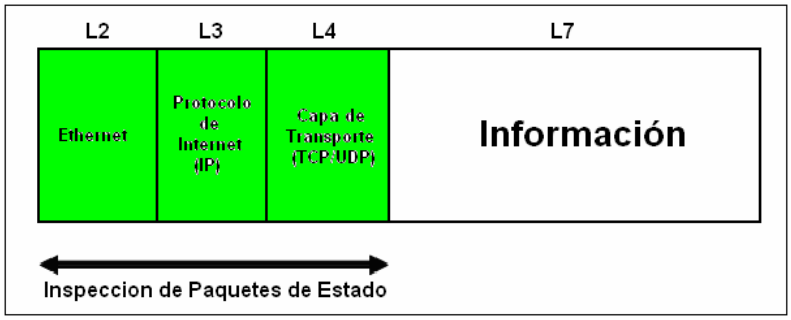


Figura 1.13 Paquete ethernet y la aplicación de Stateful Inspection

Con respecto a la utilización de reglas de filtrado, estas se pueden hacer de manera similar a un router de filtrado de paquetes, siendo estas mucho menos complejas que configurar una aplicación nueva para un firewall utilizado como Proxy. Sin embargo por lo mismo, se requieren realizar pruebas exhaustivas de las aplicaciones a utilizar para no dejar agujeros de seguridad al descubierto. De igual manera cabe mencionar que las reglas de seguridad

pueden ser implementadas en cualquiera de las capas que en las que esta tecnología realiza comparación, es decir desde la capa de red hasta la capa de aplicación.

1.4.2 Análisis de paquetes.

Esta tecnología de análisis, depende en gran medida de la negociación de tres vías que realizan el trafico TCP. Es decir, cuando un cliente inicia una nueva conexión, envía un paquete con el bit SYN establecido en la cabecera de paquetes, considerando un paquete nuevo para cada paquete con el bit de SYN activado. Si el servicio que el cliente esta solicitando esta activo en el firewall, el servicio de respuesta de paquetes SYN establece en el paquete el bit ACK. El cliente entonces responde con un paquete en que solo el bit ACK se fija, identificándolo como paquete establecido o de conexión existente.

De la forma anterior únicamente permitirá la entrada a paquetes de sesión iniciada, por los puertos establecidos únicamente para esa sesión; mientras se finaliza el envió de paquetes establecidos ningún paquete ajeno a esta conexión podrá filtrarse por el firewall, restringiendo así el acceso a paquetes ajenos enviados por posibles hackers. Esta tabla esta compuesta generalmente por la dirección y el puerto origen, luego por la dirección y el puerto destino, a continuación la IP en cuestión, seguido del estado del paquete y el tiempo que la conexión ha estado establecida. Esto se observa en la figura 1.14.

Por lo antes mencionado, se requiere que el firewall mantenga una tabla de sesiones TCP activas. Por otro lado para las sesiones UDP se crea y almacena datos de contexto sobre una conexión virtual o pseudo conexión, la cual consiste en que si un paquete de respuesta se genera y envía de vuelta al peticionario original, se establece una conexión virtual y se permite al futuro paquete de respuesta atravesar el cortafuegos. La información asociada a una conexión virtual se guarda durante un periodo de tiempo muy corto y si no se recibe dicho paquete de respuesta durante este, la conexión es invalidada. Algunos modelos de este tipo de cortafuegos pueden realizar controles similares a este sobre el protocolo ICMP.

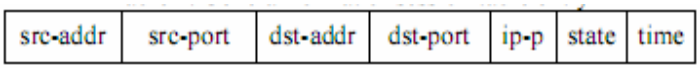


Figura 1.14 Visualización de la tabla para analizar paquetes.

Otra importante funcionalidad es la de permitir ciertos comandos mientras que deshabilita otros para una determinada aplicación. Así, es posible permitir un ping ICMP mientras que se deniega un Redirect o permitir un get sobre SNMP mientras que deshabilitamos los comandos set sobre el mismo protocolo.

1.4.3 Resumen.

Ventajas:

1. Protección a mayores niveles de seguridad.
2. Capacidad de identificar tramas y sus paquetes validos.
3. Soporta autenticación de usuarios.
4. Capaz de almacenar historial que luego puede ser usado como técnica de filtrado de paquetes.
5. Mayor velocidad de respuesta comparada con la de un Proxy.
6. Sistema de protección bastante granular.

Desventajas:

1 El firewall requiere mayores niveles de procesamiento.
2 Requiere de configuración más compleja en las políticas a usar.
3 No analizan los contenidos de los paquetes.

1.5 Deep Packet Inspection.

Tecnología liberada al público en los inicios del año 2004 junto con los equipos UTM, es una especie de filtrado de paquetes que utiliza los datos y/o cabecera de los paquetes para determinar si se cumplen los protocolos establecidos, si se encuentra virus, spam, intrusos o criterios predefinidos para determinar si se necesita una ruta hacia un destino diferente o simplemente para llevar consigo un registro estadístico. Junto con esta tecnología nace el IPS (Intrusion Prevention Service) el cual es de suma importancia, ya que es capaz de identificar el tráfico circulante de la red y detectar posibles anomalías en el mismo. Otorgando además capacidad de eliminar los cuellos de botella y de aplicar QoS en los segmentos de red a los que se someta a evaluación esta tecnología. En la figura 1.15 se observan los componentes de la inspección profunda de paquetes.

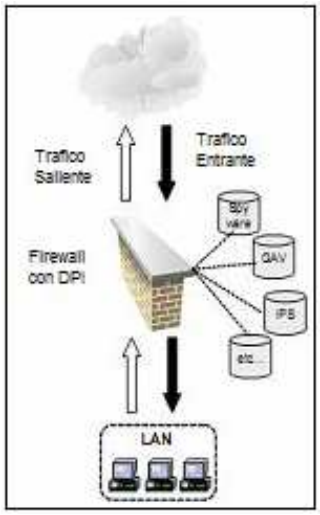


Figura 1.15 Visualización de Deep Packet Inspection.

1.5.1 Descripción

Esta técnica es capaz de realizar verificación desde la capa 2 a la capa 7 del modelo OSI, esto incluye la cabecera y la estructura de datos propiamente dicha que hasta ahora no se había mencionado en ninguna inspección anterior, esto se observa en la figura 1.16. Así mismo es capaz de identificar y clasificar el tráfico tomando como referencia una base de datos de firmas, estas se comparan con los datos extraídos del paquete permitiendo así amplio control del tráfico y más aun si se compara con el filtrado de paquetes que únicamente identificaba el encabezado. Sin embargo este tipo de inspección aun es susceptible a los ataques segmentados en paquetes.

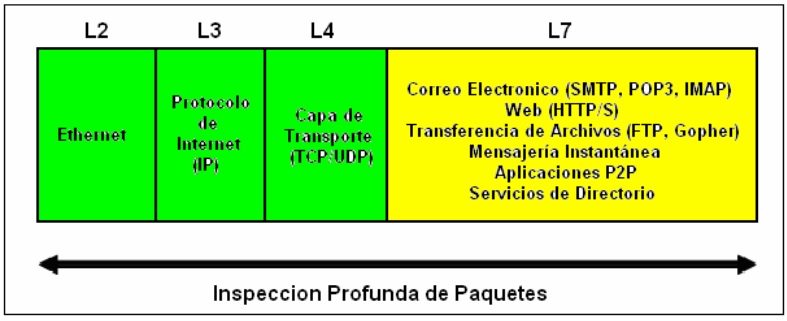


Figura 1.16 Paquete ethernet y la aplicación de Deep Packet Inspection.

El motor de inspección aplica reglas basadas en firmas que no son más que identificadores que tratan de definir por las características al tipo de trafico que se esta haciendo atravesar al firewall, las cuales a su vez utilizan motores de comparaciones, técnicas heurísticas, reglas estadísticas o técnicas para detectar anomalías, incluso se pueden realizar combinaciones de los métodos antes mencionados; para determinar la clasificación que se le da a cada paquete analizado.

Por otro lado esta tecnología tiene la capacidad de analizar y filtrar SOAP y otros mensajes XML, además de abrir y cerrar puertos dinámicamente para el tráfico de aplicaciones VoIP, realizar detección de spam, trafico de IM, e identificar las diversas formas de tráfico P2P existentes en la red.

Un paquete puede ser redirigido, marcado/etiquetado, bloqueado, de tasa limitada o clasificado de alguna manera especial de acuerdo a catalogadores en la red. Una vez se reconocen las firmas, los paquetes pueden ser tratados como flujos y no como elementos individuales para un mejor y más ágil tratamiento de los mismos. Facilitando de la misma manera la posible configuración de QoS dependiendo del tráfico que circule por la red, no solo para las redes locales, sino que también un ISP puede valerse de este método para generar el QoS para cada cliente en específico.

1.5.2 Tipos de análisis.

El análisis se realiza en base a firmas, sin embargo estas no son confiables en un cien por ciento, de hecho se recomienda mezclar las diferentes técnicas para poder clasificar de la mejor manera el tráfico circulante por la red. Lo anterior pudiese suceder cuando el patrón de comportamiento de una aplicación en específico se modifica por alguna razón, si por ejemplo se tuviera el tráfico circulante desde Internet hacia algún host, este tráfico se comportaría diferente si desde Internet pasara por un firewall y luego llegara hasta el host.

Con respecto a las diversas mezclas de análisis de tráfico que se pudieran aplicar para clasificar o identificar las diversas firmas de los paquetes podemos mencionar: análisis de puertos, similitud de cadenas, por propiedades numéricas, por comportamiento y de manera heurística.

1.5.2.1 Análisis por puerto.

Quizás es el más simple y más conocido método de análisis de paquetes; ya que las aplicaciones conocidas se comunican por medio de puertos ya establecidos, por ejemplo POP3 es usado para el correo electrónico usando el puerto 110 como puerto de entrada o el puerto 25 como puerto de salida, presentando en ambos casos en las respuestas puertos aleatorios. Sin embargo existen aplicaciones que manejan aleatoriamente el puerto de origen y el de respuesta; siendo poco recomendable la utilización de esta técnica para los casos antes mencionados, por lo que se hace necesario utilizar alguna de los otros métodos de identificación de tráfico.

1.5.2.2 Similitud de cadenas

Este método involucra la búsqueda de secuencias de caracteres alfanuméricos en los paquetes. Además estas cadenas pueden consistir de varias cadenas distribuidas en un solo paquete o consistir de varios paquetes.

Algunas aplicaciones aun declaran sus nombres en sus propios protocolos, como por ejemplo el Kazaa, donde la cadena "Kazaa" se puede encontrar en el campo de agente usuario, ya con esto se tiene una herramienta más para la clasificación de los paquetes, ya que si únicamente se verificara el número de puerto que se utiliza existirían grandes posibilidades que se considerara únicamente como trafico HTTP. La estructura de un paquete típico que utiliza Kazaa para la comunicación se muestra en la figura 1.17.

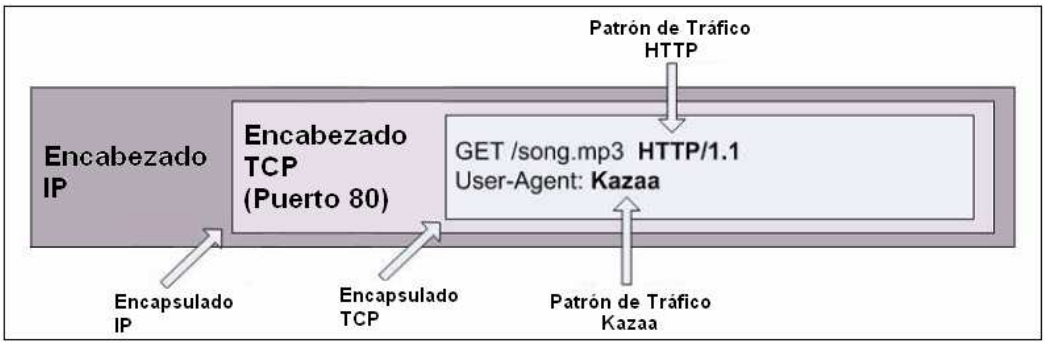


Figura 1.17 Cadena de Kazaa utilizada para el análisis de similitud de cadena

1.5.2.3 Análisis de propiedades numéricas

Este tipo de análisis involucra la investigación de características aritméticas y numéricas de cada paquete, entre ellas se pueden mencionar la longitud de paquete, número de paquetes enviados en respuesta en una transacción específica y el número de compensación de cadena en cada paquete.

Por ejemplo, se considera un proceso de establecimiento de una conexión TCP usando protocolo UDP en Skype. El cliente envía un mensaje de 18 bytes esperando una respuesta de 11 bytes. Esto es seguido por un mensaje de envío de 23 bytes, esperando una respuesta de 18, 51 o 53 bytes. Se presenta en la figura 1.18 una ilustración del caso antes mencionado. Sin embargo, este análisis exhaustivo muchas veces es aun insuficiente para dar respuestas acertadas al tráfico analizado.

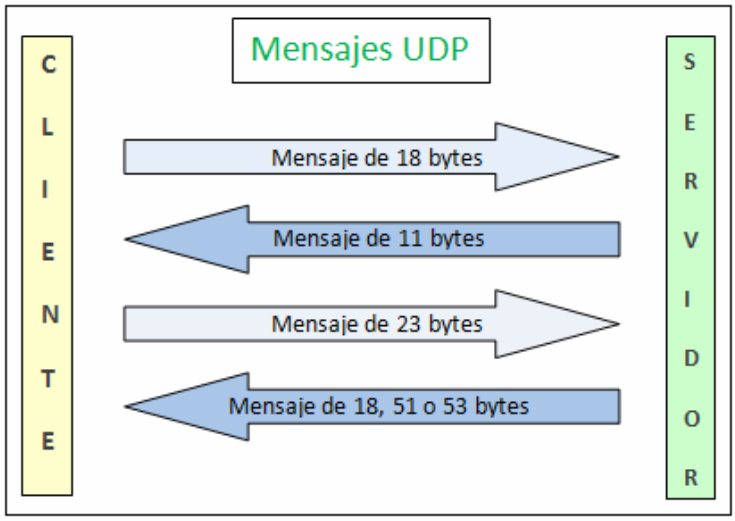


Figura 1.18 Análisis de propiedades numéricas para un tráfico de Skype.

1.5.2.4 Análisis por comportamiento y de manera heurística.

El análisis por comportamiento se refiere a la manera en que un protocolo opera. El análisis heurístico se refiere a la extracción de parámetros estadísticos de los paquetes examinados. A menudo el análisis por comportamiento y heurístico se combinan para una mejor evaluación.

En la figura 1.19 se presenta un ejemplo de comportamiento heurístico y de análisis de comportamiento, se compara tráfico HTTP con tráfico P2P. Si el histograma de longitud del paquete (PDF) es examinado sin tomar en cuenta si es tráfico de subida o bajada, se

observa que únicamente se tiene trafico HTTP en paquetes de gran longitud a una tasa de transferencia baja, mientras que el trafico de P2P tiende a la utilización de paquetes de longitud más corta a una tasa de transferencia alta; de esta manera, mediante el examen de algunos métodos estadísticos, es posible concluir si una conexión vía puerto 80 lleva el tráfico HTTP puro u otro tipo de tráfico como el tráfico de P2P.

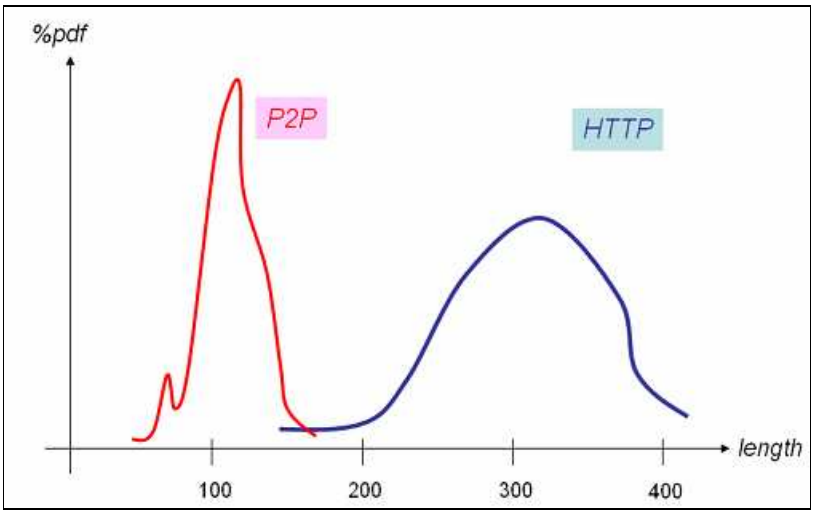


Figura 1.19 Tráfico HTTP y trafico P2P analizados por comportamiento y de forma heurística

Ventajas:

1. Extensos recursos en la evaluación de tráfico que permiten identificar con veracidad el tipo de tráfico que circulante.
2. Inspección profunda de paquetes.
3. Facilidad para complementarse con las técnicas de inspección antes mencionadas.
4. Configuración granular del equipo permitiendo flexibilidad de políticas.
5. Debido a que inspecciona todo el tráfico circulante por la red, almacena todos los logs posibles.

Desventajas:

1. Requiere una alta capacidad de procesamiento.
2. Configuración compleja.

1.6 Software Firewalls & Hardware Firewalls.

Antes de empezar a describir las diferencias entre ambos equipos es importante aclarar que una red o un equipo bien protegido ante las vulnerabilidades típicas y las amenazas de Internet, es aquel que cuenta tanto con un firewall por software como por un firewall por hardawe, debidamente actualizados ya que para ambos casos es necesario contar con las ultimas amenazas conocidas y los últimos sistemas de protección desarrollados. También es importante aclarar que la función de ambos equipos es la misma, recibir, analizar paquetes y tomar decisiones en base al contenido de estos, sin embargo como se vera a continuación esto se realiza de manera diferente.

1.6.1 Firewalls por Software

Los firewalls en software también llamados firewalls personales, son más recomendables para los usuarios domésticos ya que con sus características sencillas: de bloquear pop up, bloquear spyware, antivirus, antispam, bloqueo de contenido nocivo a menores, filtro de contenido Web, control de acceso a funciones especificas como imprimir documentos, acceder a determinados documentos, con su interfaz gráfica configurable de manera sencilla y poco moldeable a los intereses de cada usuario; se recomiendan más para este tipo de usuarios.

Una de las principales desventajas que para que estos equipos funcionen bien se necesita que estén instalados en todos los equipos que componen la red interna, así como que se tiene que tener cuidado con el tipo de software que se instala ya que podría consumir demasiados recursos de la computadora donde se haya instalado o pudiera ser incompatible con alguna versión de sistema operativo; de hecho un buen firewall por software deberá de correr en segundo plano y utilizar pocos recursos para no limitar el desempeño del host respectivo.

Por otro lado el análisis que se hace del tráfico de salida de la red interna a la red externa, suele ser más completo que el que realiza un firewall por hardware. Además es de vital importancia la actualización del sistema operativo tanto así como la actualización del software para tener un mejor funcionamiento del host protegido, también es importante asegurarse que los recursos que el software usara estarán disponibles en el ordenador usado.

Entre los fabricantes de estos dispositivos podemos mencionar: Norton, Panda, NOD32, AVG, McAfee, Trend Micro, AntiVir, Avast, etc. En la figura 1.20 se presentan logos de firewalls por software.

Figura 1.20 Fabricantes de firewalls por software.

1.6.2 Hardware

Los firewalls en hardware generalmente tienen un costo monetario más alto que las versiones en software, esto en parte debido a que son capaces de sustituir a un router y además presentan las características típicas de un firewall que antes se mencionaban como filtrado de contenido web, antispam, antivirus, IPS, IDS, control de aplicaciones, autenticación de usuarios, capacidad de realizar caché, almacenamiento de registros, todo esto de una manera diversificada presentando maleabilidad con respecto a la configuración de aplicaciones diferentes para varios usuarios desde el mismo equipo de seguridad. Es de aclarar que estos funcionan únicamente como dispositivos de seguridad periférica y algunos de ellos presentan aplicaciones extras como la capacidad de generar VPN, soportar VLAN'S.

Dependiendo del fabricante se puede contar con software propietario el cual hace difícil la violación de la seguridad del mismo, sin embargo de igual manera pueden existir dispositivos con softwares conocidos en su interior comúnmente Linux. La funcionalidad de estos últimos equipos se da desde dispositivos que en su interior asemejan a una PC con memoria flash, discos duros, etc. otros equipos no utilizan discos duros sino que únicamente memoria flash con circuitos electrónicos de alta velocidad desde donde se almacena la información, estos circuitos son llamados ASIC (Application Specific Integrated Circuit) los cuales controlan funciones especificas de aplicaciones en particular, como por ejemplo el cifrado necesario para generar VPN y SSL, además con ellos se evitan las posibles fallas que los dispositivos mecánicos (discos duros) pudieran causar.

Algunos puntos en contra se mencionan a continuación, uno de ellos es que estos dispositivos de seguridad únicamente se utilizan como dispositivos de seguridad perimetral restringiendo las amenazas de una red exterior a una interior. También que la adaptabilidad y las actualizaciones de este tipo de dispositivos pueden llegar a ser complejas, debido a que no siempre las actualizaciones de los softwares son compatibles con todos los modelos de dispositivos existentes y que además estas actualizaciones pueden liberarse con demasiado tiempo de retraso con respecto a las nuevas amenazas o técnicas de seguridad. Sin embargo esto último varía entre cada fabricante.

Entre los fabricantes de dispositivos firewalls por hardware tenemos: Cisco, Sonicwall, Fortinet, Juniper, Check Point, Barracuda, Systemantic, etc.

1.6.3 Proxy.

La mayor similitud entre dispositivos UTM y dispositivos por software se da con los proxies que son aplicaciones que se instalan sobre sistemas operativos conocidos como Windows o en su mayoría Linux para el cual ya se han desarrollado distribuciones especificas para tal uso. El término de proxy hace referencia a un programa o dispositivo generalmente una PC que realiza una acción en representación de otro.

Estos se colocan al igual que un UTM antes de la salida hacia internet es decir como aplicaciones de protección periférica pudiendo funcionar como ruteadores o como bridge, según sea la necesidad, obviamente se requiere de al menos una PC con dos interfaces Ethernet para lograr hacer la pasarela entre Internet y la LAN.

Generalmente se pueden configurar de la misma manera que un UTM, ofreciendo características muy similares como filtrado de contenido web, IDS e IPS, VPN, control de acceso de usuarios, aplicación de políticas y generación de reportes. Aunque sin la versatilidad y la efectividad que da un dispositivo por hardware, estos suelen ser funcionales para sitios que no requieran un estricto control de la LAN, que no necesiten una aplicación robusta o muy costosa ya que muchos de ellos son aplicaciones un tanto más económicas que los UTM.

Entre las aplicaciones que se desempeñan como proxies tenemos: Microsoft ISAServer, Dans Guardian, Untangle, Websense. En la figura 1.21 se muestran la configuración y el logo de un proxy que cumplen las características antes mencionadas.

Figura 1.21 Ilustración de un proxy

Capitulo 2: Introducción.

En el siguiente capítulo se presenta la descripción de los aplicativos que es posible realizar en los dispositivos UTM, mencionando los métodos comúnmente utilizados por estos dispositivos para lograr realizar dichos controles de tráfico, así mismo se presentan ilustraciones de secciones de estos equipos utilizadas con un fin en especifico.

Se ha realizado una clasificación de ocho categorías con el fin de visualizar por separado cada uno de ellos, separándolos en base a la función de cada sección. Las categorías se presentan de la siguiente forma:

- Control de acceso web
- IPS
- VPN
- Anti Spam
- Anti Spyware
- Anti Virus
- IM & P2P
- Reportes

Cabe mencionar que el estudio se realizo sin tener como guía un modelo especifico de equipo, sino más bien en base a las características que comúnmente son presentadas por estos equipos.

2.0 DESCRIPCION DE DISPOSITIVOS UTM

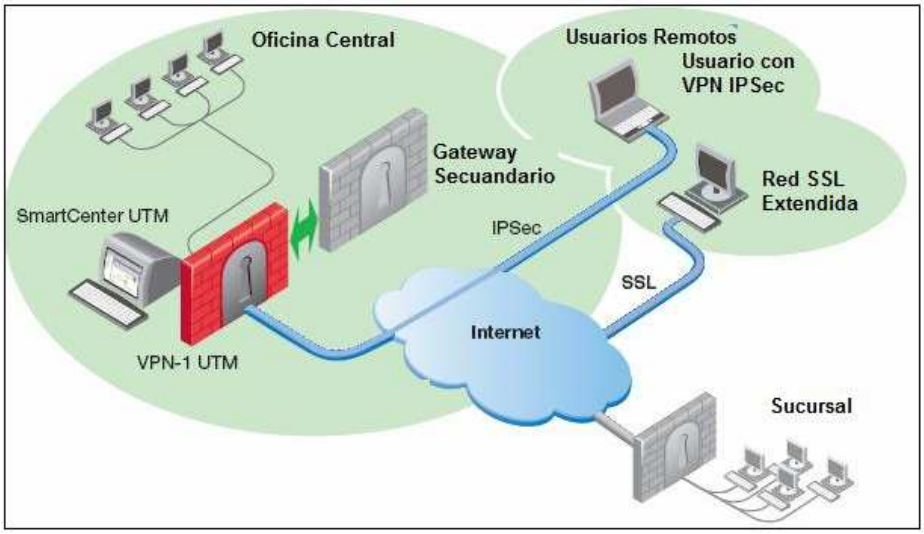


Figura 2.1 Esquema de dispositivos UTM

Los dispositivos integrados de seguridad UTM, son elementos robustos que integran tanto el hardware de conexión como un sólido sistema operativo, sobre el cual se colocan diversos bloques de seguridad. La estructura exacta depende de cada fabricante, y también puede variar en cada modelo, pero entre las más comunes tenemos el firewall o la protección contra intrusiones y otras consideradas opcionales como antivirus, anti-spam, VPN. Es decir, lo necesario para contar con una buena línea de defensa perimetral de la empresa, en la figura 2.1 se presenta una configuración típica de dispositivo UTM con algunas de las utilidades antes mencionadas.

El origen del término UTM (Unified Threat Management) se le otorga a Charles Kolodgy de la IDC (Internacional Data Corporation) en el año 2004, dicho termino es usado para describir firewalls que tienen la capacidad de desempeñar múltiples funciones extra que a los dispositivos de seguridad tradicionales no se les incluían, entre ellas se pueden mencionar filtro de contenido web, antivirus, anti-spam, IDS e IPS[1]. Todo lo anterior está relacionado íntimamente con la función de proxies que estos dispositivos utilizan analizando y enrutando todo el trafico de la red, aunque de igual manera estos pueden funcionar de modo transparente (es decir no realizar ruteo) sin utilizar totalmente a plenitud sus capacidades.

[1] http://www.wikipedia.org, consultada en abril de 2008

Los sistemas de gestión unificadas de amenazas (UTM), se han convertido en un importante elemento para garantizar la protección perimetral de cualquier empresa por pequeña que esta sea. En lugar de aplicar varios elementos diferentes para lograr las diversas capas de protección para la parte de conexiones al exterior, resulta más eficaz, compacto, y con ello barato, colocar un elemento que agrupe la mayoría, o todas las funciones necesarias o al menos a las más importantes.

El empleo de un dispositivo de seguridad ofrece la indudable ventaja de usar un hardware idóneo, normalmente reducido al mínimo, y colocar el software específico destinado a cubrir diversos aspectos de seguridad. En lugar de emplear un PC, o un servidor, convencional y montar sobre el mismo un sistema operativo estándar y luego diversas aplicaciones de seguridad, un dispositivo parte de un circuitería reducida, en la que se excluye todo elementos que puedan causar fallos o dejar abiertas puertas no deseadas.

La centralización de los elementos de seguridad en un solo dispositivo presenta grandes ventajas, aunque también algún inconveniente. Por ejemplo, se concentra toda la seguridad y conectividad en un solo elemento, con el inconveniente que si este falla, todo el sistema de seguridad se cae, e incluso todas las conexiones quedan interrumpidas. Para paliar este efecto hay diversas soluciones, como la colocación de una pareja de elementos, uno activo y otro en reserva o en balanceo de carga entre ambos que permite que el dispositivo que funciona absorba directamente la carga del que falla o está siendo sustituido. Lo anterior se conoce como HA (High Availability).

La gestión de estos equipos es un punto importante. Cuanto más centralizada y simple, más rápido, económico y fiable es crear una adecuada defensa. Además de contar con una combinación de hardware y software especializada, con sus cualidades de potente y fiable, es obligatorio que la gestión sea sencilla. La composición de los diversos elementos de seguridad que se colocan sobre un determinado dispositivo es notablemente amplia y varía mucho para cada fabricante e incluso dependiendo de gamas o modelos. El elemento más básico es un cortafuegos o firewall, que es el elemento primordial para establecer una defensa perimetral de red. Luego, capa sobre capa, se colocan otras funciones, como antivirus, anti-spam, detección de vulnerabilidades y filtrado selectivo de contenidos Web.

Una de las grandes ventajas del uso de un dispositivo es que se libera a los host finales de gran parte de la carga de trabajo en las funciones de seguridad. Al menos para todos los que están conectados dentro de la oficina. Un dispositivo de esta clase no elimina la necesidad

de contar con protección en cada puesto de trabajo, pero descarga a éstos de gran parte de su trabajo.

En la actualidad, el robo o suplantación de identidad así como el robo de tarjetas de crédito son elementos muy notables de la vulnerabilidad de seguridad informática. De lo anterior la necesidad de estar protegidos, o al menos sentirse así, ha llevado según reportes de IDC (Internacional Data Corporation) a las personas alrededor del mundo a invertir más en productos de seguridad (Antivirus, Web Filtering, IDS e IM) desde el año 2004 con unos $ 4.2 billones al año 2008 con $ 7.5 billones[2].

Para este caso, el capitulo que recién iniciamos tiene por objetivo describir de manera general, las partes que conforman un UTM sin tomar como referencia ninguna marca, modelo o fabricante en especifico.

2.0.1 Firewall.

Sin duda la parte central del dispositivo, la cual también es llamada primera línea de defensa, utiliza en los UTM la tecnología de Deep Packet Inspection como técnica de análisis de contenido con las características mencionadas en el capitulo anterior. Los actuales firewalls para empresas por pequeñas que sean SOHO (small office - home office) integran tecnologías de VPN y de control de acceso, que emplean protocolos de autenticación estandarizados y algunos UTM permiten autenticación de usuarios contra bases de datos comúnmente usadas para este fin como por ejemplo el Windows Active Directory.

La inspección de paquetes es la función principal de los firewalls, porque incluso los usuarios autenticados pueden generar tráfico malicioso, muchas veces sin saberlo. Las direcciones IP de origen y de destino, los números de puertos de origen y destino, los números de secuencia de paquetes y otros datos como el patrón de tráfico son recopilados durante sesiones de red y conservados para futuros análisis de tráfico. Dependiendo del equipo usado, si se cuenta con controles más granulares estos pueden conceder o denegar el acceso a recursos y aplicaciones basándose en la identidad del usuario, el horario del día o la información de la red.

[2] http://www.fortinet.com, consultado en abril de 2008

Los firewalls se utilizan en toda la infraestructura de la empresa para impedir que los usuarios puedan acceder a segmentos de red que tengan requisitos de seguridad únicos. Los más completos firewalls pueden controlar múltiples segmentos virtuales, proporcionando niveles de seguridad en la LAN más granulares, facilitando así la visibilidad de la red deseada a cada usuario de acuerdo a normas establecidas o a necesidades propias de la empresa o institución.

2.1 Filtrado de Contenido Web.

Quizá la parte visible más utilitaria de los UTM (al menos en un inicio) por la misma función que esta desarrolla, es la parte de Web Content Filtering (WCF) o filtrado de contenido web. Es la primordial de las aplicaciones o al menos con la que se logra percibir en mayor grado la necesidad y utilidad que puede llegar a tener un administrador de red de un dispositivo UTM, esto es porque lo que primero salta a simple vista, entre las quejas de los administradores de red más comunes tenemos:

- Pérdida de productividad, usuarios distraídos de sus labores a lo largo del día.
- Congestión de la red, ancho de banda saturado sin mayor utilización en temas de trabajo.
- Aumento de costos, muchas veces se tiene que incrementar el ancho de banda para intentar mejorar el desempeño de la red.
- Exposición a amenazas en la web (virus, gusanos, troyanos, etc.)
- Responsabilidad legal, empleados que acceden a material prohibido por la ley y que pudiera ocasionar daños a la imagen de la empresa.

En este punto es fácil pensar en las millones de páginas webs que están al alcance de los usuarios con solo tener acceso a la red pública, las cantidades de páginas improductivas entre ellas las de entretenimientos, de juegos, de noticias del espectáculo, de descargas, P2P, etc. que además de hacer improductivas u ociosas los días de los empleados, pueden convertirse en amenazas para el desempeño de la misma red, saturando o usando buena parte del ancho de banda.

Entre los sitios que generalmente se desea tener control al acceso de parte de los usuarios, están los sitios de chat, sitios pornográficos, sitios de hacking, sitios de música, aplicaciones P2P, sitios de juegos, sitios de videos en línea, etc. Para lo anterior se mencionaran al menos tres métodos de los más usados para este fin:

- *Lista de palabras prohibidas*: este método crea un diccionario con las palabras o frases prohibidas. Las URL's y el contenido web es comparado con el listado controlando de esta manera los sitios. En el inicio, esta tecnología fue usada grandemente para que los propios usuarios depuraran y afinaran su lista, el proveedor solo entregaba una lista básica la cual era manipulada al gusto de cada cliente, lo cual era un proceso largo y engorroso ya que se requería actualización manual de cada palabra. Con el tiempo, este método ha ido cambiando a tal grado de contar con listas de millones de palabras o frases. Las actualizaciones siguen siendo realizadas manualmente y el filtrado de precisión puede ver afectadas a categorías específicas, como por ejemplo los sitios de investigación médica son a menudo bloqueados ya que se les confunde con material ofensivo.

- *Bloqueo de URL:* este método utiliza prohibidas o sospechosas URL's agregadas por el administrador de red para controlar el acceso a páginas web especificas. Esta técnica igual puede ser proporcionada por el fabricante con un listado básico para que el usuario la valla puliendo de acuerdo a sus necesidades, de hecho se pueden realizar la mezcla de lista de palabras prohibidas con bloqueo de URL para tener un campo más amplio de acción.

- *Bloqueo por categorización:* es la más reciente tecnología de filtrado de contenido web que simplifica enormemente el proceso de gestión del contenido web. Este utiliza servidores externos (generalmente propietarios de cada fabricante) que ayudan a mantener cualquier sitio sospechoso actualizado apoyándose en la categorización que los servidores web con bases de datos de las URL; sin embargo estas bases de datos por motivos de memoria y robustez de equipos no está almacenada en cada dispositivo, sino lo que se hace es consultar a estas bases de datos que se encuentran almacenadas en servidores en sitios con IP públicas para que puedan ser accedidos desde cualquier sitio en Internet, y en base a esto determinar si la página a la que se está queriendo acceder está permitida o no; dependiendo del resultado encontrado si la página es accesible o no por los usuarios, esta información puede guardarse en cache para mejorar el performance de la red. La ventaja de esta tecnología es que las bases de datos se mantienen actualizadas en todo momento, eliminando la necesidad de gestionar y actualizar manualmente las listas o bases de datos contra las que se compara.

- *Integración de búsqueda segura:* algunos fabricantes añaden a la capacidad de sus equipos la integración de filtrados de contenidos de motores de búsqueda tanto de contenido Web como de imágenes, por ejemplo son capaces de interconectarse con Google, Yahoo y MSN para dar un servicio más complejo. En este caso se reescriben las búsquedas que el usuario desea realizar en base a las restricciones que cada sitio tenga habilitadas.

Algunos fabricantes, manifiestan que sus categorizadores web almacenan en su interior la información de decenas de millones de URL's y que con el día a día se van actualizando haciendo mayores esas bases de datos, así mismo el papel de seleccionar el tipo de URL que queremos que se tenga o no acceso debe de ser lo más amigable posible para el usuario y es aquí donde se da la diferencia entre algunos de ellos. Una visualización más clara de un categorizador de páginas web que el usuario podría observar se presenta en la figura 2.2

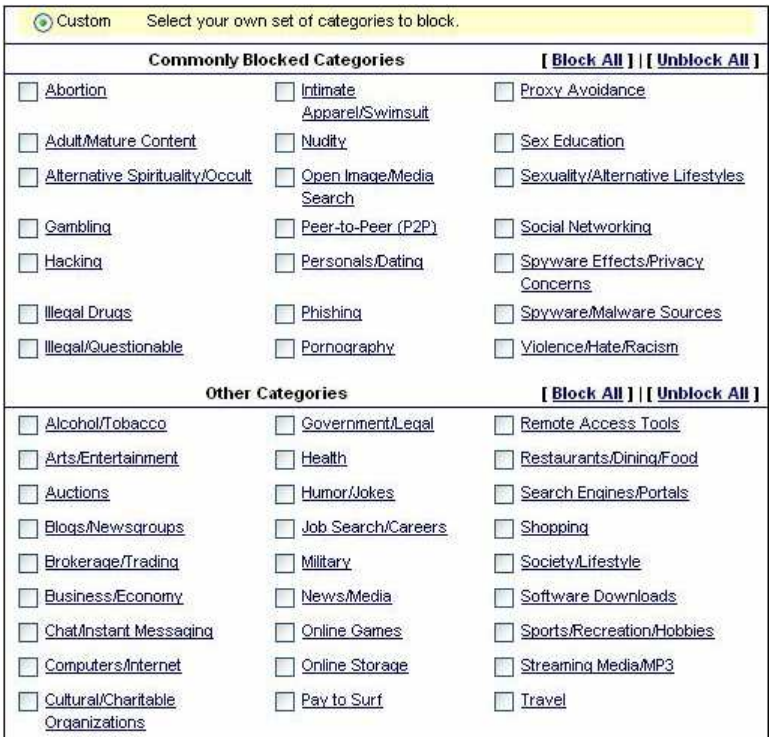


Figura 2.2 Visualización de Categorizador Web[3].

[3] http://www.bluecoat.com, consultado en abril de 2008

Además de la categorización antes mencionada, es posible también bloquear los pop-up y controles ActiveX para todas las maquinas de la red a la cual se está protegiendo, de la misma manera es posible restringir el acceso a aplicaciones en especial, por ejemplo a la capacidad de descargar archivos desde Internet de cualquier tipo, también se podría restringir descargas de algún tipo en especifico de archivos, o de alguna página web en especifica, esto dependiendo de las necesidades que se tenga.

Una ilustración mejor de los riesgos que se corren al dejar libres a los usuarios de navegar en Internet, se describe en breve, esto sucedió en el año 2004 y se le conoció como Download.Ject o ataque de JS/ Scob, el cual consistía en que después que los usuarios visitaban cierta página web, estos eran infectados con un programa, que el usuario sin saberlo, descargaba e instalaba y luego el programa se auto ejecutaba (conocida como aplicación backdoor) en sus computadoras, luego este programa estaba diseñado para que cuando el usuario visitara lugares financieros capturara toda la información posible y esta se enviara al correo electrónico de su creador, para proceder a vaciar las cuentas de ahorro personales o empresariales a las que hubiesen tenido acceso los usuarios.

Observándose la importancia de mantener actualizado el listado de palabras, URL's o bases de datos existentes, a la hora de tener bien protegida la red y con acceso restringido desde la misma, por otro lado, muchos fabricantes suelen colocar en sus dispositivos las primeras dos tecnologías mencionadas para el control de tráfico web por cualquier ajuste o página especifica que se quiera restringir o bloquear el acceso a necesidad propia de cada cliente, a esto hay que agregarle que una misma página web puede ser permitida a un gerente y bloqueada a un contador es decir dependiendo de los privilegios de cada usuario, los equipos UTM deberían de realizar esto sin mayores complicaciones y como valor agregado almacenar algún tipo de log que posteriormente se pudieran verificar.

2.2 Prevención de Intrusos.

La historia sobre los sistemas IDS (Intrusion Detection System) inicia en 1972 cuando James Anderson perteneciente a las fuerzas armadas americanas publica un texto sobre la seguridad en los ordenadores. Este tema comienza a tomar fuerza con el desarrollo de la informática y las aplicaciones críticas que a su vez se iban desarrollando. A tal grado que

entre 1984 y 1996 se desarrolla el primer modelo de IDS llamado IDES (Intrusion Detection Expert System) el cual estaba basado en reglas[4].

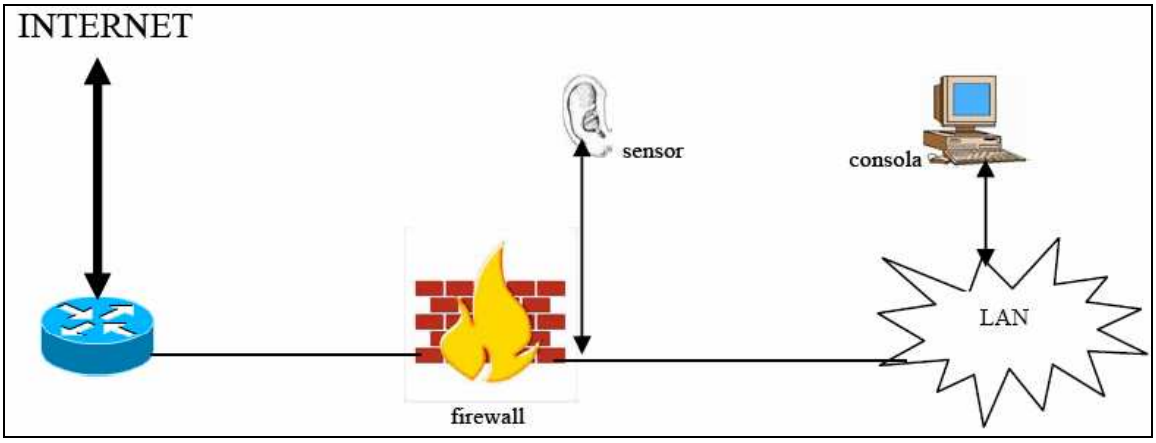


Figura 2.3 Ilustración de un firewall con sistema IDS

La parte de IDS/IPS (Intrusión Detection/Prevention System) ha ido evolucionando en respuesta a las amenazas a nivel de aplicación, con configuraciones adaptadas a sitios remotos, implementaciones periféricas y CORE de la red, se presenta una ilustración de un sistema con IDS y firewall incluido. Algunos dispositivos integran la prevención de intrusos de perfiles de aplicaciones y de red para proporcionar a los administradores de red un informe totalmente actualizado de la actividad de la red.

Es importante mencionar la diferencia entre sistemas IDS e IPS, en un inicio se introdujo el término IDS que como su nombre lo indica únicamente servía para detectar las posibles anomalías que pudiesen estar afectando a la red en donde este estuviese colocado para que el administrador de la red o persona encargada tomara acciones para evitar posibles problemas que se pudieran generar a raíz de esto, posteriormente se hizo necesario no solo identificar sino más bien tomar acciones definidas contra las anomalías detectadas, fue así que nació el término IPS utilizado para además de detectar las posibles amenazas para bloquear las mismas.

Se puede averiguar que aplicaciones se está utilizando con una IP determinada, con quien o quienes se está comunicando y qué tipo de trafico se mueven entre los host involucrados. Con información tan detallada, se puede implementar de forma sencilla un sistema de

[4] Seguridad en Redes IP, autor Gabriel Verdejo Álvarez

prevención de ataques en línea y evitar el proceso de ensayo y error inherente a las soluciones típicas.

En un inicio antes que aparecieran los sistemas IDS, se utilizaban técnicas de análisis exhaustivos de los logs de los firewalls, tratando de interrelacionar los eventos existentes. El problema de este procedimiento es que en un sistema muy accedido, el tamaño de los logs es enorme. Para tener una idea se realizara una comparación con los métodos antes mencionados y los actuales IDS, para muestra basta decir que un ataque de escaneo de puertos, en el log del firewall generaría unas 65000 entradas (64k puertos posibles) mientras que en el IDS se reflejara un solo evento: “escaneo de puertos”. Lo mismo ocurrirá en el caso de una inundación o ataque SYN, en el log aparecerían 10,000 conexiones SYN, mientras que en el IDS solo se tendría un evento: “ataque SYN”.

Los IDS suelen conformarse mediante un sistema de gestión centralizado y agentes o monitores remotos que se encargan de analizar el tráfico en los puntos remotos de la red en los que están ubicados. La comunicación entre los agentes y el gestor no se realiza a través del protocolo SNMP como ocurre en los entornos de gestión de red, sino que la comunicación se establece de forma más segura, con métodos de autenticación y codificación.

De la misma manera, la seguridad de estos sistemas se incrementan al trabajar las interfaces por las que se realiza la monitorización en modo pasivo, es decir, no actúan como destino de ningún trafico ya que no disponen de dirección IP, por lo que un atacante no puede detectar su existencia.

Algunos de los sistemas IDS existentes como por ejemplo NFR (Network Fligth Rocorder, Scanlogd, IPPL o Snort); disponen de la detección de rastreos basados en ping (ping sweep). De la misma manera, el control de estos reconocimientos se puede llevar a cabo determinando los paquetes ICMP permitidos en cada segmento de red: paquetes echo, reply, host unreachable y time exceded. A su vez, a través del control del tráfico en los routers de los bordes de la red se puede mitigar la obtención de información basada en ICMP, como la franja horaria o la máscara de subred empleada.

Estos sistemas vigilan la aparición de anomalías en el tráfico de la red, identificando variaciones en el protocolo que podrían indicar un ataque entrante, o bien tráfico saliente desde un equipo infectado. Las soluciones que supervisan los puntos vulnerables del

protocolo en lugar de las firmas específicas de ataques son más potentes porque pueden detectar nuevas amenazas y variantes de las amenazas ya existentes.

2.2.1 Tipos de Ataques más Comunes

A continuación se mencionan algunos de los ataques a los que se expone cualquier red que no esté debidamente protegida:

a) Sniffing

Un ataque realmente efectivo, ya que permite la obtención de gran cantidad de información sensible enviada sin cifrar, como por ejemplo los usuarios, direcciones de mail, números de tarjetas de crédito, etc. es emplear sniffers en entornos de red basados en difusión. El análisis de la información transmitida permite a su vez extraer relaciones y topologías de redes y organizaciones.

Los sniffers operan activando una de las interfases de red del sistema en modo promiscuo, de esta forma, el sniffer almacenara logs del tráfico que circule por la tarjeta de red, ya sea destinado o generado por el propio sistema o desde/hacia cualquiera de los sistemas existentes en el entorno de red compartido. Asimismo, pueden ser instalados tanto en sistemas como en dispositivos de red por los mismos usuarios.

Generalmente para el funcionamiento de los sniffers es necesario tener acceso a un sistema interno de la red, haciendo un tanto más complicado este proceso si se quisiera realizar desde el exterior. Una vez ya instalado el sniffer, este pudiese ser utilizado para averiguar cuentas de correo, cuentas de banco, todo eso con su respectivo passsword, creando complicaciones para los usuarios y empresas víctimas.

b) IP spoofing

Se basa en actuar en nombre de otro usuario tal y como si fuese el mismo. En TCP/IP se basa en la generación de paquetes IP con una dirección origen falsa o distinta a la del origen del ataque, esto con el fin de obtener información deseada de la víctima.

c) DoS: Denial of Service

Un ataque de denegación de servicio se centra en sobrepasar los límites de recursos establecidos para un servicio determinado, obteniendo como resultado la eliminación temporal del servicio. Por ejemplo, si un servidor es capaz de procesar 10 peticiones por

segundo, y se le envían 30, parte del tráfico legítimo no recibirá servicio, o incluso, puede que la saturación del tráfico provoque que el servidor deje de responder a ninguna petición. Los destinos de estos ataques suelen ser objetivos visibles, como servidores Web, DNS o Routers.

Este tipo de ataques no supone ningún peligro para la seguridad de las maquinas, ya que no modifica los contenidos de información, ni permite obtener información sensible. Simplemente persiguen entorpecer el acceso de los usuarios a los servicios de un sistema. Normalmente, una vez que el ataque finaliza, se vuelve a la situación normal; aunque en algunas ocasiones este ataque se utiliza únicamente como cortina de humo para llevar a cabo ataques de mayor dimensión.

d) Net Flood

El objetivo de este ataque es degradar la capacidad de conexión a la red de un sistema, saturando sus enlaces de comunicaciones. Por ejemplo, si el enlace de una organización dispone de un ancho de banda de 20Mb y un atacante dispone de un enlace de 100Mb, prácticamente la totalidad del tráfico cursado por la organización pertenecerá al atacante, por lo que no podrá enviarse tráfico útil.

Para lograr estos altos anchos de banda, puede recurrirse a la obtención de múltiples sistemas desde los que pueda efectuar el ataque o apoderarse de sistemas mal administrados y protegidos que posean redes de gran capacidad.

e) DDoS

Una variante de DoS son los DDoS, o ataques de denegación de servicios distribuidos, que se basan en realizar ataques DoS de forma masiva a un mismo objetivo desde diferentes localizaciones de la red, de forma que la potencia de ataque sea mucho mayor.

El modo de operación genérico de las herramientas DDoS es: el intruso se comunica mediante comandos con un elemento denominado handler; este se encarga de gestionar el registro, realizando previamente, de un conjunto de agentes, normalmente elevado en número, que son realmente el origen de los paquetes DDoS. Por tanto, los agentes y el handler conforman una red de ataque, que actúa en el momento en que el handler retransmite a todos y cada uno de los agentes las órdenes invocadas por el intruso remotamente.

Las comunicaciones entre estos elementos se realizaban originalmente por puertos fijos y a la larga conocidos, por lo que este método de funcionamiento podría ser detectado por sistemas IDS con facilidad.

f) Ping of Death

Conocido como ping de la muerte, este ataque se basa en enviar un paquete de ping de un tamaño muy grande; teniendo en cuenta que el tamaño máximo de paquete en TCP/IP es de 64Kbytes, la implementación de la pila TCP/IP asigna un buffer en memoria de este tamaño. En el caso de que la información sea mayor, el buffer puede desbordarse. El resultado obtenido en muchas ocasiones es que el sistema destino deja de proveer servicio al bloquearse, ya sea reiniciándose o apagándose. Lo que sucede realmente es que el paquete emitido es fragmentado, a nivel IP, en las redes intermedias, los fragmentos van siendo encolados en el sistema destino hasta que se reciben los últimos pedazos (un paquete de 65536 bytes es suficiente), que son los que desbordan el buffer, provocando un comportamiento anómalo.

g) Troyanos

Esta vulnerabilidad en numerosas ocasiones es empleada para introducir servicios TCP/IP no deseados en sistemas destino y poder así ejecutar ataques remotos posteriormente o incluso tomar su control por completo. También son conocidos como backdoors, son fragmentos de programas no autorizados que se introducen en otros para que el programa original ejecute ciertas acciones no deseadas.

En el caso de Troyanos que afectan a TCP/IP muchas veces para entender su comportamiento se suele realizar una comparación con programas completos que normalmente se justifican como herramientas de administración remota y acceso remoto, que facilitan el acceso y completo control del sistema destino, ejemplo PCAnywere, VNC, Windows Terminal Services, etc.

Generalmente este tipo de software se descarga en los sistemas al visitar alguna página web o servicio electrónico público sin que el usuario se percate de ello. Las consecuencias y acciones de cada herramienta pueden variar en función de la idea con que se diseñaron ya que pueden actuar como fuente de ataques DDoS o incluso manipular y extraer información del sistema que les hospeda.

2.2.2 Técnicas usadas en IDS e IPS

A continuación se mencionan las diversas técnicas de verificación de tráfico usadas por sistemas IDS/IPS para la identificación de amenazas:

- *Verificación de la lista de protocolos:* algunas formas de intrusión como el ping de la muerte o escaneo silencioso de TCP utilizan violaciones de los protocolos IP, TCP, UDP e ICMP para atacar un equipo; una simple verificación del protocolo puede revelar paquetes no validos.

- *Verificación de protocolos de la capa de aplicación:* algunas formas de intrusión emplean comportamientos de protocolos no validos. Para detectar eficazmente estas intrusiones un IDS verifica si el comportamiento para cada protocolo en la capa de aplicación identificado es el "correcto". Esta técnica no necesita examinar la base de datos de firmas en su totalidad basta con revisar secuencias de bytes en particular por lo que se considera una técnica rápida, además es eficiente ya que elimina algunas falsas alarmas.

- *Reconocimiento de ataques (comparación de patrones):* esta es la técnica más frecuentemente usada. Consiste en la identificación de una intrusión al examinar un paquete y reconocer, dentro de una serie de bytes, la secuencia que corresponde a una firma especifica. Esta técnica se puede refinar si se combina con una sucesión o combinación de indicadores TCP. Esta técnica presenta ventajas como la poca generación de falsas alarmas además de diagnosticar rápidamente un ataque específico; sin embargo este necesita ser actualizado continuamente.

- *Análisis Heurístico:* detecta la existencia de "trafico anómalo", sin embargo es necesario dejarlos un tiempo "aprendiendo o reconociendo" el tráfico que generalmente se transfieren por la red, este método es efectivo ya que detecta cualquier cambio en la red, sin embargo necesita de una configuración especializada para no generar falsos positivos.

- *Detección de anomalías:* se centra en identificar comportamientos inusuales en un host en una red, sin embargo la configuración de este requiere que sea muy específico para no generar falsas alarmas sino en cambio aporte a la base de datos de firmas existentes en caso de ser un ataque no agregado a la misma.

Por otro lado, dependiendo del fabricante pueden afrontar y denegar los ataques que se producen durante el peligroso periodo del "día cero". El ataque del Día Cero se define como los ataques nuevos o desconocidos para los cuales no se escribió un parche o una firma. Por lo que la protección del día cero de define como: "la ventana de vulnerabilidad que se genera entre el periodo que se lanza un nuevo ataque y que el administrador de red actualiza su equipo en contra de esta"[5]. Una mejor ilustración de esto se presenta en la figura 2.4.

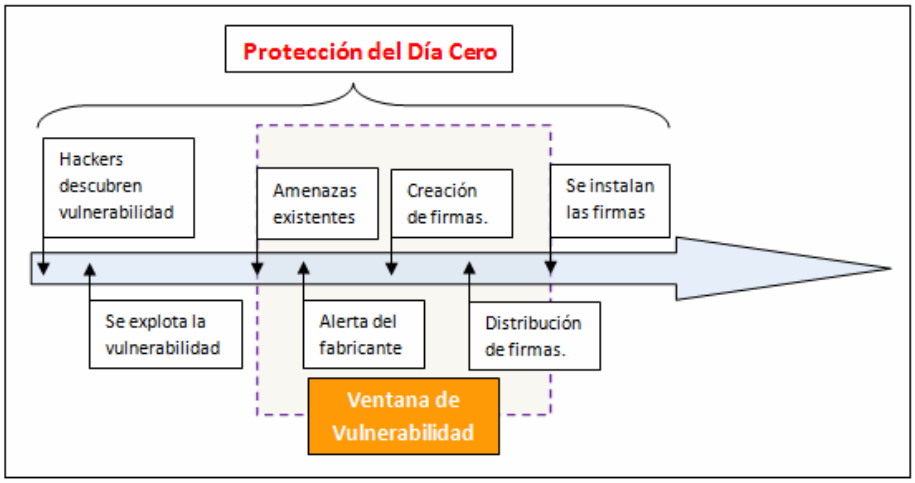


Figura 2.4 Ilustración de la protección del Día Cero

Dependiendo del fabricante del dispositivo y de la técnica usada como IDS, puede existir un método que permita el control de diversas vulnerabilidades, disponiendo de la posibilidad de detectarlas y también de responder a ellas generando una alarma, descartando el paquete o reseteando la conexión.
Otros sistemas más avanzados son capaces de modificar de forma dinámica las listas de control de acceso en los dispositivos en el momento de detectarse el ataque, con el objetivo de filtrar el tráfico asociado al mismo.

Las formas más comunes para contagiarse sin esta ser la intención del usuario con algún tipo de programa malicioso son:

- Utilizando los servicios de libre intercambio de archivos o de descarga gratuita (shareware, freeware, etc.).
- Abriendo mail's infectados.

[5] http://www.watchguard.com, consultado en abril de 2008

- Accediendo a las invitaciones de los pop-up.
- Visitando sitios inseguros.

Al llegar a este punto, es necesario recordar que la forma en como se configuran los IDS tiene que llevar una mezcla de generalidad y particularidad, ya que si se realizan las configuraciones de manera muy general se activaran fácilmente falsas alarmas y si se realizan de manera muy particular se pudiera dejar pasar muchas amenazas existentes, he aquí lo necesario de un adecuado balance entre la generalidad y la particularidad, además de conocer con certeza el tipo de trafico que se circulara en la red.

2. 3 Redes privadas virtuales.

Uno de los servicios adicionales más valorados de los UTM es la posibilidad de construcción de redes privadas virtuales (VPN) que permiten extender a las comunicaciones externas la seguridad del interior de nuestra red. Estas VPN se construyen en la cúspide de la pila de capas existentes en la red usando protocolos adicionales y fuertes cifrados con mecanismos de control de integridad, sustitución o repetición de la información transmitida. En la Figura 3.5 se muestra la ilustración de una VPN.

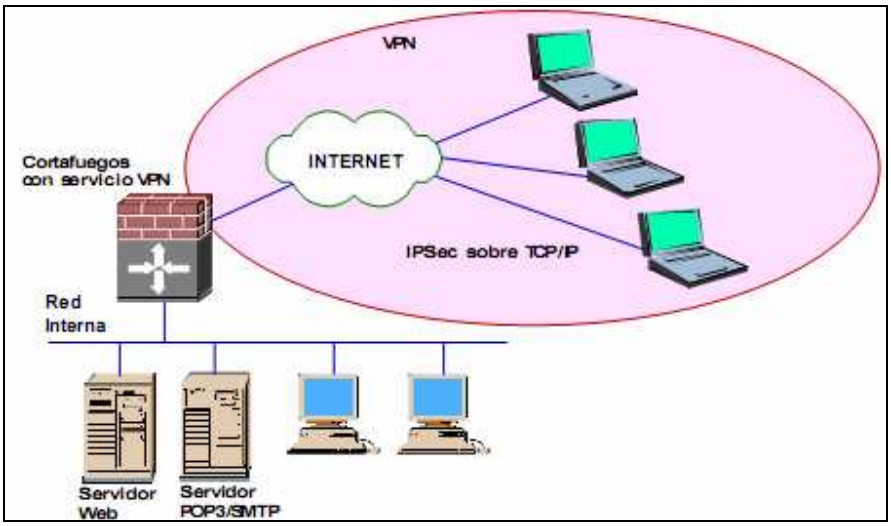


Figura 2.5 Ilustración de una VPN

2.3.1 Características.

Entre las ventajas del uso de VPN tenemos:

- Utilización de estándares de seguridad reconocida: IPSec y SSL.
- Interoperabilidad entre fabricantes.
- Integración con otras tecnologías como DSL, RDSI, IDS.
- Accesos remotos seguros desde cualquier punto como si se estuviera en la oficina.
- Reducción drástica de costes de comunicaciones.

Para hacer posible la comunicación de manera segura es necesario proporcionar los medios para garantizar la autenticación, integridad y confidencialidad de toda comunicación:

- *Autenticación y autorización:* identificación del usuario/equipo y su nivel de acceso.
- *Integridad:* la garantía de que los datos enviados no han sido alterados. Para ello se utiliza funciones Hash que son algoritmos usados para generar claves que representen de manera única a documentos, archivos o usuarios; los algoritmos Hash-as comunes son los Message Digest (MD2 y MD5) y el Secure Hash Algorithm (SHA).
- *Confidencialidad:* dado que los datos viajan a través de un medio potencialmente hostil como Internet, los mismos son susceptibles a intercepción, volviéndose fundamental el cifrado de los mismos. De este modo, la información no debe poder ser interpretada por nadie más que los destinatarios de la misma. Se hace uso de algoritmos de cifrado como Data Encryption Standard (DES), Triple DES (3DES) y Advanced Encryption Standard (AES).

Existen tres arquitecturas básicas de conexión VPN:

a) VPN de acceso remoto

Es el modelo más usado actualmente y consiste en usuarios móviles o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hotel, etc.) utilizando Internet como vinculo de entrada a su LAN. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa.

b) VPN punto a punto

Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vinculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los

servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicional, sobre todo en las comunicaciones internacionales, también llamada tecnología de túnel o tunneling.

c) VPN interna WLAN

Esquema menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del acceso remoto pero en vez de utilizar Internet como medio de conexión, emplea la misma red local de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas.

2.3.2 Tipos de VPN

La VPN se usa para codificar las comunicaciones que deben cruzar un medio no confiable, usualmente Internet. Las VPN pueden ser de diversas características dependiendo del dispositivo, pueden ser PPTP, SSL o IPSec. De las tres antes mencionadas, la menos recomendada y por lo mismo la menos usada es la VPN PPTP (Point to Point Tunneling Protocol) ya que es la más vulnerable a ataques por su misma estructura y cuyo código ya ha sido descifrado, esto quizás en parte por ser el protocolo estándar propuesto por Microsoft. En la figura 3.6 se muestra los niveles de seguridad de IPSec y SSL.

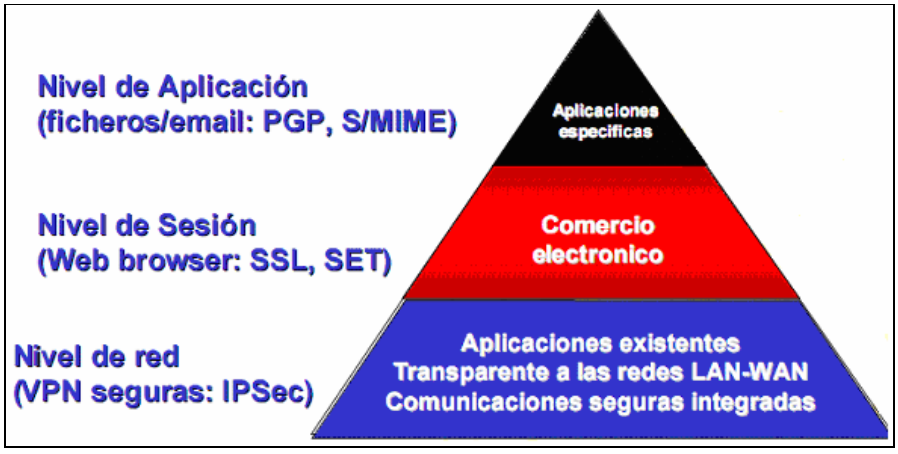


Figura 2.6 Niveles de operación de IPSec y SSL

2.3.2.1 VPN IPSec

La VPN IPSec (IP Security) es un conjunto de estándares desarrollados por el IETF (Internet Engineering Task Force) destinado a solventar las deficiencias de seguridad de TCP/IP, proporcionando mecanismos fiables de autenticación, confidencialidad e integridad en las comunicaciones; por otro lado proporciona conexiones de acceso punto a punto o remotas y asumen que los usuarios tendrán acceso a todos los recursos de la red. Un gran avance de IPSec es que los ajustes en la seguridad se pueden gestionar sin necesidad de realizar cambios individualmente en todos los host.

IPSec utiliza el intercambio de claves, este intercambio es llamado IKE (Internet Key Exchange), es usado para obtener una clave maestra para la autenticación, sin embargo esta autenticación puede ser basada en una clave pre-compartida o basada en cifrado asimétrico (emplea certificados digitales).

IPSec proporciona cifrado a nivel de la capa de red, es decir IP convirtiéndose en una solución transparente a las aplicaciones. De hecho este protocolo originalmente fue diseñado para IPv6, migrándose luego a IPv4 siendo hoy en día uno de los protocolos más usados por los fabricantes de UTM para implementar las VPN, ya que proporciona protecciones contra la repetición de tramas y gracias a su ubicación en la pila de protocolos, es capaz de trabajar con UDP y otros protocolos de la capa de transporte.

En IPSec, mediante el uso de fingerprints o huellas en los paquetes IP, generados a través de una función Hash basada en el uso de una clave compartida por ambos extremos de la comunicación, se asegura la identificación (autenticación) del emisor, por lo que permite erradicar la técnica de IP Spoofing. Así mismo soluciona otros problemas de seguridad, además de la autenticación, como los ataques de DoS y los problemas de confidencialidad o privacidad basándose en el cifrado, y la integridad de los datos intercambiados mediante funciones Hash.

Por otro lado, los protocolos de cifrado requieren una utilización mucho mayor de CPU, para ejecutar los algoritmos asociados a estos procesos, por lo que facilitan la ejecución de ataques DoS. La utilización de tarjetas específicas de cifrado libera al CPU general de este proceso, pero simplemente desplaza el punto débil asociado al consumo de procesamiento a otro componente. Esto hecho ha dado lugar a que no se empleen en IPSec firmas digitales completas.

IPSec dispone de dos servicios:

- *AH (Autentication Header):* asegura la autenticación y la integridad de los datagramas enviados entre dos sistemas, protegiendo la cabecera del paquete IP de spoofing, detrás de esto va una cabecera adicional que contiene una función Hash (HMAC) segura para permitir la validación de la información que contiene el paquete, permitiendo que únicamente las partes que conocen el cifrado puedan tener acceso al datagrama.
- *ESP (Encapsulation Security Payload):* asegura confidencialidad, autenticación e integridad de datos, flujo de tráfico confidencial mediante análisis de tráfico. Para este caso se utilizan cifradores de bloque; por otro lado HMAC solo tiene en cuenta la carga del paquete, la cabecera IP no se incluye dentro de su proceso de cálculo. Por lo que para este caso el uso de NAT se podría utilizar aunque este sigue siendo un tanto incompatible con IPSec.

2.3.2.1.1 Características de IPSec

IPSec puede utilizarse como:

- Modo transporte: para cifrar directamente el tráfico entre dos equipos, es el host el que genera los paquetes, solo se cifran los datos, la cabecera queda intacta; se añaden pocos bytes; permite ver las direcciones de origen y destino. Las capas de transporte y aplicación están siempre aseguradas por un hash, de forma que no pueden ser modificadas de ninguna manera. Se utiliza en comunicaciones entre dos host.
- Modo túnel: comunicación entre dos subredes, que puedan usarse para comunicación segura entre dos redes corporativas, se cifra el paquete IP completo dentro de otro datagrama IP, para el sistema final es transparente. El modo túnel se utiliza para comunicaciones red a red (túneles seguros entre routers, para VPNs) o comunicaciones ordenador a red u ordenador a ordenador sobre Internet.

En la figura 2.7 se ilustran la estructura de los paquetes.

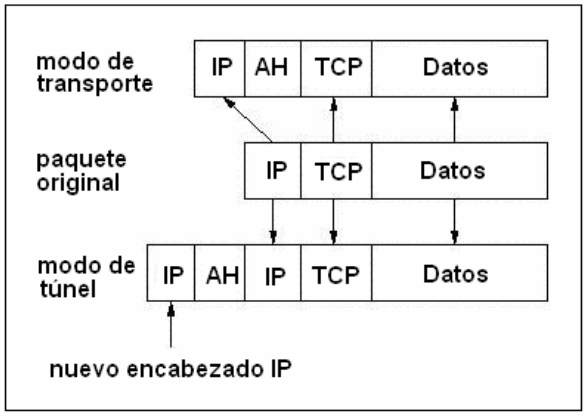


Figura 2.7 Estructura de paquetes en modo transparente y túnel.

Para proteger la integridad de los datagramas IP, los protocolos IPsec emplean códigos de autenticación de mensaje basados en resúmenes (HMAC – Hash Message Autentication Codes). Para el cálculo de HMAC se emplean algoritmos de resumen como MD5 y SHA para calcular un resumen basado en una clave secreta y en los contenidos del datagrama IP. El HMAC se incluye en la cabecera del protocolo IPSec y el receptor del paquete puede comprobar HMAC si tiene acceso a la clave secreta.

Para proteger la confidencialidad de lo datagramas IP, los protocolos IPsec emplean algoritmos estándar de cifrado simétrico. El estándar IPsec exige la implementación de NULL y DES. En la actualidad se suelen emplear algoritmos más fuertes: 3DES, AES y Blowfish.

Para protegerse contra ataques por denegación de servicio, los protocolos IPsec emplean ventanas deslizantes. Cada paquete recibe un número de secuencia y sólo se acepta su recepción si el número de paquete se encuentra dentro de la ventana o es posterior. Los paquetes anteriores son descartados inmediatamente. Esta es una medida de protección eficaz contra ataques por repetición de mensajes en los que el atacante almacena los paquetes originales y los reproduce posteriormente.

Para que los participantes de una comunicación puedan encapsular y desencapsular los paquetes IPsec, se necesitan mecanismos para almacenar las claves secretas, algoritmos y direcciones IP involucradas en la comunicación. Todos estos parámetros se almacenan en asociaciones de seguridad (SA - Security Associations). Las asociaciones de seguridad, a su vez, se almacenan en bases de datos de asociaciones de seguridad (SAD - Security Asocciation Databases).

2.3.2.2.2 Funcionamiento de IPSec

Cada asociación de seguridad define los siguientes parámetros:

- Dirección IP origen y destino de la cabecera IPSec resultante. Estas son las direcciones IP de los participantes de la comunicación IPSec que protegen los paquetes.
- Protocolo IPSec (AH o ESP).
- El algoritmo y la clave secreta empleados por el protocolo IPSec.
- Índice de parámetro de seguridad (SPI). Número de 32 bits que identifica a la asociación de seguridad.

En una asociación de seguridad se definen las direcciones IP de origen y destino de la comunicación. Por ello, mediante una única SA sólo se puede proteger un sentido del tráfico en una comunicación IPsec full duplex. Para proteger ambos sentidos de la comunicación, IPsec necesita de dos asociaciones de seguridad unidireccionales.

Las asociaciones de seguridad sólo especifican cómo se supone que IPsec protegerá el tráfico. Para definir qué tráfico proteger, y cuándo hacerlo, se necesita información adicional. Esta información se almacena en la política de seguridad (SP - Security Policy), que a su vez se almacena en la base de datos de políticas de seguridad (SPD - Security Policy Database).

Una política de seguridad suele especificar los siguientes parámetros:

- Direcciones de origen y destino de los paquetes por proteger. En modo transparente estas serán las mismas direcciones que en la SA. En modo túnel serán distintas.
- Protocolos y puertos a proteger. Algunas implementaciones no permiten la definición de protocolos específicos a proteger. En este caso, se protege el tráfico entre las direcciones IP indicadas.
- La asociación de seguridad a emplear para proteger los paquetes.

La configuración manual de la asociación de seguridad es proclive a errores, y no es muy segura. Las claves secretas y algoritmos de cifrado deben compartirse entre todos los participantes de la VPN. Uno de los problemas críticos a los que se enfrenta el administrador de sistemas es el intercambio de claves: ¿cómo intercambiar claves simétricas cuando aún no se ha establecido ningún tipo de cifrado?

Para resolver este problema se desarrolló el protocolo de intercambio de claves por Internet (IKE - Internet Key Exchange Protocol). Este protocolo autentica a los participantes en una primera fase. En una segunda fase se negocian las asociaciones de seguridad y se escogen las claves secretas simétricas a través de un intercambio de claves Diffie Hellmann. El protocolo IKE se ocupa incluso de renovar periódicamente las claves para asegurar su confidencialidad

2.3.2.2.3 El protocolo IKE

El protocolo IKE resuelve el problema más importante del establecimiento de comunicaciones seguras: la autenticación de los participantes y el intercambio de claves simétricas. El protocolo IKE suele implementarse a través de servidores de espacio de usuario, y no suele implementarse en el sistema operativo. El protocolo IKE emplea el puerto 500 UDP para su comunicación.

El protocolo IKE funciona en dos fases. La primera fase establece un ISAKMP SA (*Internet Security Association Key Management Security Association*). En la segunda fase, el ISAKMP SA se emplea para negociar y establecer las SAs de IPsec. La autenticación de los participantes en la primera fase suele basarse en claves compartidas con anterioridad (PSK - Pre-shared keys), claves RSA o certificados digitales X.509.

La primera fase suele soportar dos modos distintos: modo principal y modo agresivo. Ambos modos autentican al participante en la comunicación y establecen un ISAKMP SA, pero el modo agresivo sólo usa la mitad de mensajes para alcanzar su objetivo. Esto, sin embargo, tiene sus desventajas, ya que el modo agresivo no soporta la protección de identidades y, por lo tanto, es susceptible a un ataque *man-in-the-middle* (por escucha y repetición de mensajes en un nodo intermedio) si se emplea junto a claves compartidas con anterioridad (PSK). Pero sin embargo este es el único objetivo del modo agresivo, ya que los mecanismos internos del modo principal no permiten el uso de distintas claves compartidas con anterioridad con participantes desconocidos. El modo agresivo no permite la protección de identidades y transmite la identidad del cliente en claro. Por lo tanto, los participantes de la comunicación se conocen antes de que la autenticación se lleve a cabo, y se pueden emplear distintas claves pre-compartidas con distintos comunicantes.

En la segunda fase, el protocolo IKE intercambia propuestas de asociaciones de seguridad y negocia asociaciones de seguridad basándose en la ISAKMP SA. La ISAKMP SA

proporciona autenticación para protegerse de ataques *man-in-the-middle*. Esta segunda fase emplea el modo rápido.

Normalmente, dos participantes de la comunicación sólo negocian una ISAKMP SA, que se emplea para negociar varias (al menos dos) IPsec SAs unidireccionales.

Las relaciones entre dos equipos que desean hablar mediante el protocolo IPSec vienen caracterizadas por el conjunto de parámetros que define todos los aspectos a tener en cuenta, como los algoritmos de autenticación y cifrado, la longitud de las claves, el servicio (AH o ESP) a emplear. Este conjunto de parámetros se conoce como SA, Security Association.

2.3.2.2 VPN SSL

Concepto desarrollado por Netscape en 1994, el cual en esta primera versión no tuvo versión comercial y rápidamente se migro a la versión 2.0, sin embargo la versión que dio el reconocimiento que en la actualidad cuenta este protocolo es la versión 3.0 desarrollada en 1996. Este ha sido aprobado por instituciones financieras para el comercio electrónico. Sin embargo, no fue hasta su tercera versión, conocida como SSL V3.0 que alcanzo su madurez, superando los problemas de seguridad y las limitaciones de sus predecesores[6].

En su estado actual SSL proporciona los siguientes servicios:

- *Cifrado de datos:* la información transferida, aunque caiga en manos de un atacante, será indescifrable, garantizando así la confidencialidad.
- *Autenticación de servidores:* el usuario puede asegurarse de la identidad del servidor al que se conecta y al que posiblemente envié información confidencial.
- *Integridad de mensajes:* se impide que modificaciones intencionales o accidentales en la información mientras viaja por Internet pasen inadvertidas.
- *Autenticación del cliente (opcional):* permite al servidor conocer la identidad del usuario, con el fin de decidir si puede acceder a ciertas áreas protegidas.

Las VPN SSL establecen una sesión codificada entre un navegador y una aplicación. Las principales características que han hecho que SSL sea aceptado y reconocido como una aplicación casi estándar para el comercio electrónico y las comunicaciones seguras sobre Internet es la facilidad de implantación por parte de los administradores de red y lo transparente que resulta esta aplicación para el usuario.

[6] SSL y Otros Protocolos Seguros, upm.es consultado en abril de 2008

2.3.2.2.1 Características de SSL

SSL proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de la criptografía. Generalmente solo el servidor es autenticado, mientras que el cliente no se autentica, la autenticación mutua requiere un despliegue de infraestructura de claves públicas (PKI) para los clientes. SSL permite aplicaciones cliente-servidor para prevenir escuchas, falsificación de identidad y mantener la integridad del mensaje.

SSL aplica una serie de fases básicas:

- Negociar entre las partes el algoritmo que se usará en la comunicación.
- Intercambio de claves publicas y autenticación basada en cifrados digitales
- Cifrado del tráfico basado en cifrado simétrico.

El rasgo que distingue a SSL de otros protocolos para comunicaciones seguras, es que en el modelo OSI se ubica entre capa de transporte y aplicación al igual que HTTP, FTP, SMTP, telnet, etc. En la figura 2.8 se observa la estructura y ubicación del protocolo SSL en donde se observan las dos capas y los cuatro componentes con los que cuenta.

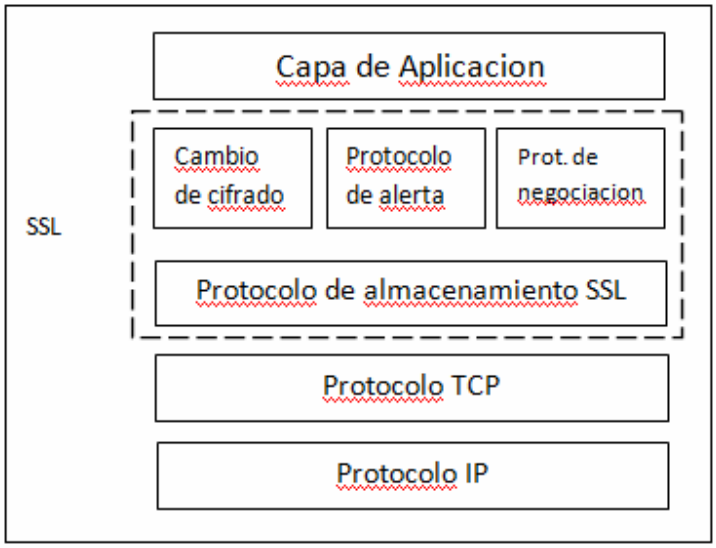


Figura 2.8 Ubicación e Ilustración del protocolo SSL

A continuación se presenta una breve descripción de las cuatro partes que componen al protocolo:

- El protocolo de registro (Record Protocol) se encarga de encapsular el trabajo de los elementos de la capa superior, construyendo un canal de comunicaciones entre los dos extremos objeto de la comunicación.
- El verdadero corazón de SSL está en el protocolo de Handshake que es el encargado de intercambiar la clave que se utilizará para crear un canal seguro mediante un algoritmo eficiente de cifrado simétrico. También es responsabilidad de este protocolo coordinar los estados de ambos extremos de la transmisión.
- El protocolo de Alerta es el encargado de señalizar problemas y errores concernientes a la sesión SSL establecida.
- Por último, el Change Cipher Spec Protocol está formado por un único mensaje consistente en un único byte de valor 1 y se utiliza para notificar un cambio en la estrategia de cifrado.

2.3.2.2.2 Funcionamiento de SSL

A grandes rasgos, SSL trabaja de la siguiente forma: en primer lugar intercambia una clave de longitud de 128 bits mediante un algoritmo de cifrado asimétrico. Mediante esa clave establecemos un canal seguro utilizando para ello un algoritmo simétrico previamente negociado. A continuación, toma los mensajes a ser transmitidos, los fragmenta en bloques, los comprime, aplica un algoritmo hash para obtener un resumen (MAC) que es concatenado a cada uno de los bloques comprimidos para asegurar la integridad de los mismos, realiza el cifrado y envía los resultados. El estado de todas estas operaciones son controladas mediante una máquina de control de estados. Una sesión SSL puede comprender múltiples conexiones. Adicionalmente, se pueden establecer múltiples sesiones SSL simultáneas[7].

Gracias a la ubicación en los modelos TCP y OSI, SSL resulta muy flexible, ya que puede servir para dar seguridad a otros servicios además de HTTP para Web, solo con hacer pequeñas modificaciones en el programa que utilice el protocolo de transporte TCP. SSL proporciona sus servicios de seguridad sirviéndose de dos tecnologías de cifrado: criptografía de clave pública (asimétrica) y criptografía de clave secreta (simétrica)

Por otro lado, este protocolo ha sido concebido para trabajar únicamente con protocolo TCP y es sumamente difícil trabajar con otros protocolos de la capa de transporte como UDP, sin embargo debido a la importancia y al uso que UDP tiene en la actualidad se han

[7] SSL y Otros Protocolos Seguros, www.upm.es consultado en abril de 2008

desarrollado soluciones eficientes que permiten su utilización. Esta consiste en levantar una sesión SSL sobre TCP y luego cifrar independientemente cada paquete UDP para que si uno de ellos no llega a su destino en la transmisión, este no influya en la comunicación; de manera que cada paquete UDP sea descifrable de forma independiente e ira cifrado con su propia clave.

Para el intercambio de los datos entre el servidor y el cliente, utiliza algoritmos de cifrado simétrico, que pueden elegirse típicamente entre DES, triple-DES, RC2, RC4 o IDEA. Para la autenticación y para el cifrando de la clave de sesión utilizada por los algoritmos anteriores, usa un algoritmo de cifrado de clave pública, típicamente el RSA. La clave de sesión es la que se utiliza para cifrar los datos que vienen del y van al servidor una vez establecido el canal seguro.

Se genera una clave de sesión distinta para cada transacción, lo cual permite que aunque sea revelada por un atacante en una transacción dada, no sirva para descifrar los mensajes de futuras transacciones. Por su parte, MD5 o SHA se pueden usar como algoritmos de resumen digital (Hash). Esta posibilidad de elegir entre tan amplia variedad de algoritmos dota a SSL de una gran flexibilidad criptográfica.

Existen soluciones VPN SSL que combinan múltiples métodos de acceso en un solo dispositivo, proporcionando máxima seguridad y amplias posibilidades de acceso. El más simple es el acceso base sin clientes, que emplea funciones SSL existentes en los navegadores web, clientes de correo electrónico y dispositivos móviles estándar. Una segunda opción es la tecnología basada en agentes, que permite acceder mediante un navegador a las aplicaciones cliente/servidor. Una tercera opción también está basada en agentes y proporciona niveles de acceso ilimitados tanto al personal informático como a los usuarios especiales.

Estas opciones permiten crear grupos de usuarios que satisfagan las necesidades de cada uno (empleadores, empleados, trabajadores a distancia, etc.) y a los que luego se asociaran los métodos de acceso y los controles de seguridad correspondientes. El dispositivo detecta dinámicamente el tipo de conectividad dependiendo de la ubicación del usuario, del tipo de red y del dispositivo terminal utilizado, así como de los recursos a los que el usuario necesita acceder.

Por las características antes mencionadas muchos autores presentan a IPSec como el sustituto de SSL, sin embargo otros insisten que ambos pueden coexistir juntos puesto que ofrecen soluciones distintas. En la tabla 2.1 se presenta un cuadro comparativo propuesto por Nortel Networks con respecto a ambos protocolos:

	SSL/TLS	IPSec
CONTROL DE ACCESOS		
Conexiones permanentes		☑
Conexiones efímeras o puestos móviles	☑	
Ambos tipos de acceso	☑	☑
USUARIOS		
Todos los usuarios son empleados de la compañía		☑
No todos los usuarios son empleados de la compañía	☑	
No todos los usuarios son empleados de la compañía y, además, algunos trabajan con sus propios sistemas	☑	☑
SOFTWARE CLIENTE		
Todos los usuarios han de tener acceso a todos los recursos de la red		☑
Deseamos controlar el acceso a determinadas aplicaciones	☑	
Necesitamos niveles variables de control de acceso en las diferentes aplicaciones	☑	☑
CONFIDENCIALIDAD Y AUTENTICIDAD		
Precisamos de un alto nivel de seguridad en el cifrado y autenticación		☑
La confidencialidad y autenticidad no son especialmente críticas en nuestros sistemas	☑	
Precisamos de niveles moderados de confidencialidad e integridad	☑	
CRITICIDAD DE LOS RECURSOS ACCEDIDOS		
Alta		☑
Moderada	☑	
Variable	☑	☑
NIVEL TECNICO DE LOS USUARIOS		
Entre moderado y alto		☑
Entre moderado y bajo	☑	
IMPLANTACIÓN, FLEXIBILIDAD Y ESCALABILIDAD		
Deseamos una implantación rápida y facilidad de mantenimiento	☑	
Deseamos flexibilidad en las modificaciones futuras		☑
Ambas consideraciones son importantes	☑	☑

Tabla 2.1 Cuadro comparativo entre IPSec y SSL

2.4 Anti Spam.

2.4.1 Introducción.

En la actualidad el correo electrónico es una de las aplicaciones más usada sobre Internet además del explorador web tomando una gran importancia en nuestro desempeño diario, por consiguiente el nivel de ataques existentes derivados del uso del correo electrónico ha venido incrementándose.

Cuando se envía un correo electrónico este es enviado por Internet a un servidor SMTP/ESMTP (Simple Mail Transfer Protocol / Enhanced Simple Mail Transfer Protocol) proporcionado comúnmente por el ISP (Internet Service Provider), esto se realiza utilizando el MTA (Mail Transport Agent), este busca a un servidor POP3 / IMAP (Post Ofice Protocol / Internet Message Access Protocol) asociado al dominio del correo del destinatario y a este lo envía para que sea descargado por el usuario respectivo, para este caso es necesario contar con un cliente de correo el cual es un programa que se utiliza para enviar y recibir correos, por medio del MUA (Mail User Agent). Otra forma de accesar al correo electrónico es vía web o vía HTML, usando los correos gratuitos o los mismos correos institucionales, en este último caso basta con accesar a la IP respectiva del servidor de correo para ver los correos respectivos.

En un inicio es importante definir el concepto de Malware (Malicious Sotfware) que es un software que tiene como objetivo infiltrarse o dañar un ordenador sin el consentimiento de su dueño y con finalidades muy diversas ya que en esta categoría encontramos desde un troyano, pasando por un virus hasta un spyware, estos términos más adelante se describirán más detalladamente. Esta expresión es un término muy utilizado por profesionales de la computación para definir una variedad de software o programas de códigos hostiles o intrusivos.

En esta sección empezaremos por la descripción del término spam o correo basura, este término se utiliza en los mensajes electrónicos no solicitados, generalmente de tipo publicitario los cuales son enviados en cantidades masivas a diversos usuarios. Inicialmente el correo electrónico era el único afectado con este tipo de ataques, sin embargo los niveles de acción se han extendido a teléfonos celulares, envíos de faxes, sistemas de mensajería instantánea, etc.

2.4.2 Spam

El primer registro de spam que se tiene es del 5 de marzo de 1994[8], este fue enviado por una firma de abogados de Canter and Siegel el cual en el primer día después de la publicación facturó cerca de $10,000; desde entonces el marketing mediante correo electrónico ha crecido a niveles impensados desde su creación.

Otros tipos de Spam aparte del tradicional enviado por correo electrónico:

a) Spam por mensajería instantánea:

También conocido como spim, utiliza los sistemas de mensajería instantánea como ICQ, MSN o Yahoo Messenger. Muchos sistemas de mensajería ofrecen directorio de usuarios, incluyendo información demográfica tal como edad y sexo. Los publicistas pueden reunir esta información, conectarse al sistema y enviar mensajes no solicitados.

Para enviar mensajes instantáneos a millones de usuarios de la mayoría de los servicios de mensajería instantánea solo se requiere software de scripting y los nombres de usuarios de los receptores. Los spammers también apuntan a los canales IRC (Internet Relay Chat), el cual es un protocolo de comunicación que conecta un cliente a un servidor en tiempo real basado en texto plano usado para la mensajería instantánea; utilizando los bots IRC o robot informático para el envió masivo de mensajes publicitarios.

b) Spam en grupos de noticias, blogs o foros:

A pesar que estos no son muy comunes, si existen este tipo de ataques y consiste en el envío de información o publicidad masiva a estos grupos, en donde se pueden presentar con formatos similares a la información que allí se maneja, pero con contenido totalmente diferente al que se refleja en los demás artículos de la misma.

c) Spam en telefonía móvil:

También conocida como spit, utiliza el envió de SMS a móviles, ofreciendo servicios o incitando a enviar mensajes a determinados números cortos. El origen de los teléfonos utilizados por los spammers puede ser muy variado, desde la llamada en serie números de teléfono, hasta conseguir los números de teléfono móviles por algún tipo de servicio o de contacto en páginas web, es decir la página ofrece recibir

[8] http://www.wikipedia.org, consultado en mayo de 2008

llamadas de otras personas o recibir mensajes gratuitamente a quienes se inscriban en la lista, posteriormente los números de teléfono recolectados son utilizados para la realización de spam, o incluso para la inclusión en servicios de suscripción, por los que se carga al receptor el costo de los mensajes en el peor de los casos.

En la figura 2.9 se muestra la diversidad de categorías del contenido del spam que se recibe por correo electrónico.

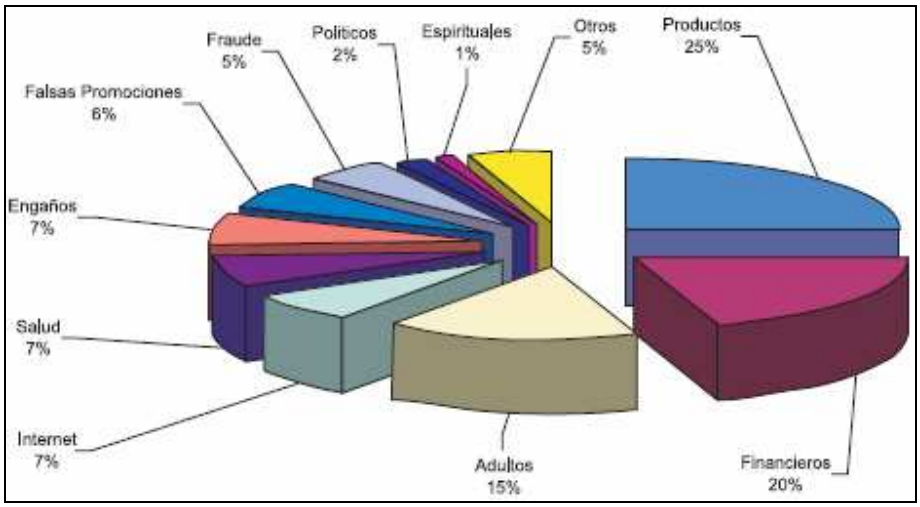


Figura 2.9 Diferentes categorías del contenido del Spam enviado por correo electrónico.[9]

Los spammers (personas o instituciones que envían spam) utilizan diversas técnicas para conseguir las largas listas de direcciones de correo que necesitan para su actividad, generalmente a través de robots o programas automáticos que recorren internet en busca de direcciones.

Algunas de las principales fuentes de direcciones para luego enviar spam son las páginas web como foros, blogs, etc.; que contienen las direcciones de correo de sus visitantes; listas de correo gratuitos las cuales se hackean alguna cuenta y se conocen los contactos de este usuario; correos electrónicos con chistes, cadenas, etc. que los mismos usuarios de internet suelen reenviar sin ocultar las direcciones, y que pueden llegar a acumular docenas de direcciones en el cuerpo del mensaje pudiendo ser capturado por algún usuario malicioso; páginas en las que se solicita la dirección de correo electrónico para acceder a un determinado servicio o descarga; compra de bases de datos de direcciones de correos a empresas o particulares.

[9] http://www.brightmail.com, consultado en abril de 2008

Una vez se cuenta con una gran cantidad de direcciones de correo validas, los spammers utilizan programas que recorren la lista enviando el mismo mensaje a todas las direcciones; además es frecuente que el spammer controle que direcciones funcionan y cuáles no, esto lo realizan registrando los mensajes que fueron abiertos usando web bugs las cuales son imágenes escondidas en el correo estas se conectan con el servidor e informan que el correo ha sido abierto, o colocando links en los correos con los cuales supuestamente se deja de recibir información de la cuenta que se envió, sin embargo esto sirve para determinar que la cuenta esta activa y que además se leyó el contenido del correo enviado.

La técnica más usada en la actualidad es la creación de troyanos que se expanden masivamente por ordenadores no protegidos (sin firewalls), de esta forma los ordenadores afectados son utilizados por el spammer como "ordenadores zombis" que envían spam a los contactos o direcciones colocadas en cadenas de los usuarios víctimas, causando que este sin saberlo ni notar alguna diferencia sea identificado como spammer por los servidores a los que él está enviando spam lo que puede conducir a que no se deje acceder a determinadas páginas o servicios. Actualmente el 40% de los mensajes de spam se envían de esta forma.

En la figura 2.2 se muestran los 10 países mayores generadores de spam, según la Unión Europea.

Pos.	Ciudad	Spam
1	Estados Unidos	25.3 %
2	China	14.1%
3	Rusia	6.8 %
4	Reino Unido	6.2 %
5	Corea del Sur	5.6 %
6	Alemania	4.5 %
7	Japón	4.2 %
8	Francia	4.1 %
9	Canadá	3.2 %
10	Otros	26 %

Tabla 2.2 Países considerados mayores generadores de spam

2.4.2.1 Métodos de Detección de Spam

Entre los inconvenientes que presenta el Spam tenemos:

- Transmitir mensajes indeseados: esto reduce el ancho de banda
- Almacenar los mensajes: usar espacio del servidor hasta tal grado de saturarlo.
- Borrar o leer los mensajes: reduce la productividad del empleado.

Entre los diversos métodos para identificar el Spam tenemos:

a) Filtrado de Contenido

Realiza comparaciones con listas de frases o palabras peligrosas, este análisis se pude usar en el asunto del mensaje, cuerpo del mensaje, etiquetas HTML o archivos adjuntos; esta técnica evita que cierto tipo de palabras y tópicos sean enviados hacia o desde los usuarios.

Sin embargo es ineficiente para controlar el Spam ya que requiere de una atención continua del administrador, por otro lado algunos trucos simples lo hacen vulnerable como sustituir “viagra” por “v*i*a*g*r*a” y el hecho de intercambiar caracteres por símbolos ya que solo reconocerá las palabras almacenadas en la base de datos, de la misma manera, no puede analizar mensajes que solo contengan imágenes y direcciones web (URL).

Por otro lado, requiere de grandes capacidades de procesamiento y tiempo para realizarlo, además de las continuas actualizaciones y las variaciones de las ya existentes.

b) RBL (Real Time Black Holes)

Es un sistema automático y distribuido que comparte listas de supuestos spammers y sus dominios o direcciones IP, sin embargo estas listas no son auditadas o supervisadas por algún ente regulador sino que son manejadas por “voluntarios”, por lo que tienden a restringir muchas veces a usuarios o ISP que no necesariamente son generadores de Spam, muchas veces la identidad de estos pudiera haber sido reemplazada por el remitente, generando lo que se conoce como falsos positivos, lo cual es muy perjudicial sobre todo si el ISP utiliza IP’s publicas alternantes entre sus clientes.

El método de listas negras consiste en mantener un listado de servidores de correo de los que se tiene constancia que envía spam, nuestro servidor de correo (MTA), al recibir una conexión, comprueba si el servidor remitente está en la lista negra o no; si está, cierra la conexión y no acepta el correo, por tanto funciona antes de la transmisión del mensaje, ahorrándose el tráfico de los correos no deseados. La forma en como estas listas funcionan pueden ser verificando el contenido del mensaje o verificando el mensaje mismo.

Los principales problemas de este método se dan cuando se enlistan a ISP completos o cuando se enlistan a servicios de correo gratuitos populares como Hotmail o Yahoo restringiendo el envió de correos, estos servidores decidieron que ellos no eran responsables del spam que se enviaran por sus cuentas, por lo tanto, forzaron a dejar de usar las listas negras a quien quisiera recibir sus correos; y es lo que sucedió perdiendo este método su eficacia.

c) Análisis Heurístico

Utiliza una técnica que evalúa varios atributos para identificar spam y asignar una calificación, esto lo hace efectivo en correos HTML de texto o con imágenes; por otro lado este debe de ser actualizado periódicamente ya que los cambios en las técnicas de envío de spam son cambiantes. Un ejemplo de regla heurística es clasificar como spam a correos con una fecha de emisión incorrecta.

En contra de esta técnica, empleada por soluciones como SpamAssassin, juega la dificultad de establecer, probar y mantener las reglas, así como la inversión de tiempo que el administrador debe emplear en mantener actualizado el sistema. Por otro lado esta técnica es muy conocida y desafiante para los spammers ya que estos prueban sus nuevos spams contra motores heurísticos para determinar si son utilizables o no.

d) Filtros Bayesianos

Sistema de aprendizaje basado en análisis estadístico de vocabulario calificando las palabras como “amenazantes” e “inofensivas”, tiene como principio que la mayoría de los sucesos son dependientes de otras variables y de que la probabilidad de que un suceso sucede en el futuro puede deducirse a partir de la ocurrencia en el pasado

del mismo. Este sistema permite el entrenamiento del sistema para diferenciar automáticamente mensajes de spam de los que no lo son.

Básicamente su funcionamiento se da con los correos que pasan el filtro, los cuales llegan a los destinatarios, luego los usuarios los marcan como spam y se devuelven al servidor, este servidor lo analiza y mediante algoritmos que implementan el teorema de Bayes se reestructura con la nueva información para intentar que los mensajes que se le parezcan no vuelvan a pasar.

Por otro lado, esta técnica es muy atacada por los spammers usando palabras "inofensivas" cifrando el Spam con código HTML. Otra técnica usada por los spammers, es usar después de mensajes de propaganda, palabras de uso frecuente colocadas aleatoriamente; de esta manera conseguían que los filtros bayesianos, al ser retroalimentados con estos correos, confundiesen algunas palabras de uso frecuente con spam, es decir haciendo que correos legítimos, que con mucha probabilidad contuviesen esas palabras, se convirtieran en 'falsos positivos' siendo estos de gran número, haciendo de estos filtros un método poco eficiente para la identificación y filtro de spam.

e) Checksums

Crea un molde de ejemplos de spam conocidos, aquí es necesario actualizar periódicamente la base de datos con datos de nuevos ataques de spam detectados, sin embargo es fácil de evitar agregando caracteres dentro del mensaje.

Este método funciona tratando los correos no deseados como si fueran virus; se busca una forma de encontrar una firma, un algoritmo que dé una serie que sea diferente para prácticamente cualquier correo, y se guarda una lista de las firmas de los correos que son considerados SPAM. Cuando el mensaje llega al MTA, este calcula su firma y la busca en la lista de firmas SPAM. Si la encuentra, rechaza el mensaje, sino lo encuentra lo procesa.

El problema de este método es el mismo que el de los virus: necesitan que alguien reciba el spam y lo notifique. Y, además desde que se recibe el primer correo no deseado, hasta que se encuentra la firma y se actualiza el filtro pueden pasar horas, y durante ese tiempo el correo va entrando. Y los correos son muchos más abundantes y variados que los virus, por tanto este problema se intensifica.

Los spammers intentan pasar este filtro haciendo que los correos 'muten', es decir, que cambien su forma, aunque no su contenido. El mensaje de propaganda lo difunden igual pero le añaden palabras aleatorias al principio y/o al final, que hacen que se tarde más en poder definir la firma representativa.
Un ejemplo de checksum es el Hash, la cual es una representación de cada mensaje, y esa base de datos contiene las funciones hash de cada mensaje enviado usando la RBL, esto permite identificar rápidamente que el mismo mensaje se está enviando a muchos servidores, y le permite advertir a futuros clientes que el mensaje es probablemente spam.

f) SpamPost

Para intentar detectar los correos no deseados antes que lleguen a un usuario se idearon los SpamPots o SapmTraps. La idea consiste en publicar direcciones de correo en sitios donde se sospecha que los spammers recogen direcciones de correo para llenar sus 'listas víctimas'. Estas direcciones no pertenecen a nadie, por tanto no deberían recibir ningún correo legítimo. Por tanto, todo el correo que se reciba será considerado spam, y se podrán crear las reglas adecuadas (firmas/bayes) para que los filtros no lo dejen pasar.

Este método no tiene ningún filtro de correo de por sí, solo permite aprender de los correos de spam de forma automática, sabiendo seguro que lo que se ha recibido es spam, pero se tiene que aplicar otros métodos para obtener resultados.

g) Listas Grises

Los spammers al observar que en la web se ha disminuido el número de los servidores open relays, han tenido que montar sus propios servidores de correo para enviar el spam, y han buscado otras maneras de ahorrarse el máximo de tráfico posible. Han recortado el protocolo SMTP, y han eliminado de los mensajes las cabeceras que han podido, y lo más importante, para acelerar el funcionamiento han hecho que durante el envió no se espere respuesta.

Normalmente cuando un servidor de correo envía un correo, espera a que el servidor destino conteste si lo ha recibido correctamente o no, y en el caso de no recibir confirmación vuelve a intentar el envío. Los spammers, como son conocedores que muchísimas de las direcciones de correo que usan como víctimas son incorrectas o

inexistentes, han encontrado que el tráfico que dedicaban a los mensajes de error era demasiado alto, y por lo tanto, la mayoría han optado por no esperar esta respuesta.

Y en este punto es en el cual se fundamenta la idea de las listas grises, la cual es mantener una lista de servidores 'familiares', de los cuales se aceptan los correos sin restricción, y hacer pasar una prueba a los 'no familiares', intentando distinguir entre la forma de actuar de un servidor de correo normal y los servidores 'recortados' de los spammers. Por lo que habiendo comprobado que un servidor 'no familiar' cumple los RFC, se le añade a la lista de 'familiares'.

Es decir, el servidor de correo mantiene una lista de tripletas conocidas que relacionan email remitente, IP remitente y dirección destino. Cuando llega un correo que tiene la tripleta que no está enlistada, el MTA le devuelve un 'Error Temporal', y se añade su tripleta a la lista, cuando el servidor de correo reciba un 'Error Temporal' tiene que reintentar el envió del correo pasado un rato.
Si el correo lo había enviado un servidor de correo válido, reintentará al cabo de un tiempo prudencial y entonces el correo se aceptara, únicamente el correo se retardara entre 5 y 30 minutos, pero a partir de este momento, siempre que este remitente envíe un correo a este destinatario a través de esta IP de servidor, el correo se aceptara sin restricciones. En caso de que sea un servidor de correo 'recortado' (como lo de los spamers), no se reintentará y por tanto no llegará nunca.

Este método es bastante nuevo, y no está muy extendido entre los servidores de correo, por tanto los spammers aún no han hecho acciones masivas para evitarlo. Por este motivo, aunque es muy sencillo y fácilmente evitable, es muy efectivo ya que aproximadamente el 90% del spam se descarta antes de su transmisión. Las ventajas son su efectividad, y que se rechazan los correos spam antes de que sean transmitidos, ahorrando el tráfico que comportan.

Como inconveniente de este método, un usuario recibe un mensaje legitimo de un remitente nuevo, el mensaje se retardara entre cinco y treinta minutos, aunque este retraso no es del todo significativo. Algunas implementaciones de spammers han conseguido detectar los emails no distribuidos, reenviándolos inmediatamente, y es por eso que las implementaciones de las listas grises han forzado que desde el primer intento hasta el segundo tenga que pasar un tiempo prudencial, es decir cinco minutos.

Como hemos podido observar ningún método es efectivo en su totalidad, sin embargo si se combinan entre ellos, pueden aprovecharse las fortalezas de cada uno y tener herramientas eficientes en la identificación y detección de spam.

2.5 Antispyware.

2.5.1 Introducción.

Los programas espía o spyware son aplicaciones que incluyen un pequeño programa o código que recopila información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas, pero también se han empleado en círculos legales para recopilar información contra sospechosos de delitos. Además pueden servir para enviar a los usuarios a sitios de internet que tienen la imagen corporativa de otros, con el objetivo de obtener información importante.

Los spyware pueden contener rutinas que capturan las teclas digitadas por el usuario denominadas keyloggers, tales como nombres de usuario, contraseñas, números de tarjetas de crédito, fecha de expiración y hasta sus códigos secretos las cuales son almacenadas en archivos de tipo "log" para posteriormente ser enviadas al intruso vía cualquier servicio de Internet.

Las bases para el spyware se iniciaron en los años ochentas con las creaciones de keylogers en los campus universitarios, de ahí en adelante se comenzaron a utilizar estos para conocer datos de los usuarios de PC's. Sin embargo el termino spyware fue usado por primera vez el 16 de octubre de 1995 por programadores de Microsoft, ya el termino como tal con el significado que conocemos actualmente, se dio origen en el año 2000 al describir las capacidades del firewall Zone Alarm. Ya para el año 2006, el spyware se había convertido en uno de las amenazas más comunes en el ámbito de las redes, sobre todo para usuarios del navegador Internet Explorer[10].

Utiliza la conexión a Internet de un usuario en un segundo plano, el llamado "canal falso" sin su conocimiento o permiso explícito. El uso silencioso en un segundo plano de una conexión a Internet por el "canal falso" requiere la divulgación verídica y completa del uso

[10] http://www.us-cert.gov, consultado en mayo de 2008

de dicho canal, seguido de la confirmación del consentimiento explícito y conocido de este uso. Si no se obtiene el permiso, el acto se considera hurto de información.

Los programas espía pueden ser instalados en un ordenador mediante un virus o un troyano que se distribuye por correo electrónico, o bien puede estar oculto en la instalación de un programa aparentemente inofensivo. Entre las anomalías que se observan en hosts al estar infectado con spyware tenemos:

- Bombardeo de ventanas pop-up
- Navegador con direcciones predeterminadas, es decir las ventanas hacia las que conduce son diferentes a las que el usuario intenta accesar.
- Cambio repentino o repetitivo de la página de inicio o página principal de navegación de su computadora.
- Aparición de barras de herramientas nuevas e inesperadas, así como aparición en el escritorio de iconos inesperados.
- Teclas que no funcionan, mensajes de error continuos, funcionamiento lento de la computadora y problemas al abrir o guardar programas.

2.5.2 Tipos de Spyware.

Existen diferentes clasificaciones de spyware, a continuación se mencionan los más representativos:

- *Secuestro de sesión en Browser:* esta clase de spyware modifica los parámetros de usuario del browser. Pueden ser instalados de varias maneras, su propósito es modificar el comportamiento del browser para que el usuario accese directamente a sitios que el autor del spyware desee y que generalmente son bloqueados por los usuarios, muchas veces el autor gana comisiones por lograr el acceso de usuarios a páginas o sitios web definidos.

- *Cookies:* son pequeñas piezas de información almacenados en un sistema de un host provenientes del uso de un servidor web. Estas son usadas para que durante las posteriores visitas, el servidor web pueda recuperar esas “cookies”, por lo general estas cookies son usadas para almacenar información de autenticación de usuario, preferencias y otro tipo de información propia del usuario. Estas se utilizan para diferenciar a un usuario de otro, pero también de la misma manera utilizando técnicas llamadas “web bugs” se pueden utilizar para dar seguimiento a un usuario

definido a través de la red y asi lograr obtener la mayor cantidad de información del usuario víctima.

- *"Web bugs"*: son elementos HTML, en formas de imágenes de etiquetas inapreciables para los usuarios (muchas veces en formatos GIF), las cuales tienen como funciones recopilar información de quien las ve o si están adjuntas en un correo de quien abre el correo almacenando la IP desde donde se leyó siendo capaz de rastrear a este mismo. Una vez se cuenta con lo anterior se pueden crear cookies que almacenen información personal de cada usuario.

- *Spyware Autónomo:* son programas espías autónomos que se ejecutan al iniciar la sesión del usuario que instalo dicho software y teniendo acceso a los recursos para este mismo usuario, esto se vuelve más crítico si el usuario infectado es el administrador o el root. Estas aplicaciones pueden realizar cualquier función de espionaje o control del host infectado.

- *Bots:* una clase especial de malware es conocida como bot o zombie el cual es uno de los mayores problemas observados en Internet. Los Bots son funciones rutinarias que podrían convertirse en controles remotos instalados en host, las cuales pueden ser accesadas por los creadores de estos spyware. Estos bots pueden formar parte de un Bonet que no es más que una mini red de host infectados y controlados por el mismo usuario remoto.
  Las funciones más comunes que incluyen los Bots son scaners de vulnerabilidad, herramientas de DDoS, la capacidad de capturar paquetes de red. Los host infectados con bots pueden ser usados como servidores proxies para generar spam, haciendo aún más difícil la tarea de rastrear a los spammers.

- *Adware:* se define como cualquier programa que automáticamente ejecuta, muestra o baja publicidad a la PC después de instalado el programa o mientras se está utilizado la aplicación. Muchos de estos programas llevan consigo código spyware que se encargan de recolectar información del usuario.

2.6 Antivirus.

Un virus informático es un programa que se copia y ejecuta automáticamente teniendo por objeto alterar funcionamiento de los host sin el consentimiento del usuario, estos incluso pueden reemplazar archivos ejecutable por otros infectados, o incluso destruir intencionalmente los datos almacenados en un host.

El funcionamiento de estos es el siguiente, el código del virus queda alojado en la memoria RAM de la computadora, aun cuando el programa que lo contenía haya terminado de ejecutarse. El virus toma entonces el control de los servicios básicos del sistema operativo, infectando luego los archivos ejecutables y finalmente se añade el código del virus al del programa infectado y se graba en disco, con lo cual el proceso de replicado se completa.

Muchas veces se tiende a confundir los términos como spyware descrito en el apartado anterior y virus descrito recientemente, sin embargo existen diferencias entre ambas definiciones, la primera hace referencia a un programa que necesita ser bajado e instalado muchas veces sin conocimiento del usuario ya que esto lo hace inconscientemente, sin embargo, los virus son aplicaciones que muchas veces se instalan sin interferencia del usuario.

El primer virus que ataco a una PC se le llamo Creeper, fue creado en 1972[11], el programa emitía periódicamente en la pantalla el mensaje: “I’m a creeper … catch me if you can” (soy una enredadera, agárrenme si pueden). Para eliminar este problema se creó el primer antivirus, denominado Reaper (segadora). Sin embargo el termino virus se adoptaría hasta 1984, pero estos ya existían desde antes. Sus inicios fueron en los laboratorios de AT&T Bell Computers, en el cual se desarrolló un juego de guerra nuclear llamado Core Wars, el cual consistía en ocupar toda la memoria RAM del equipo contrario en el menor tiempo posible.

2.6.1 Clasificación de los Virus.

Existen diversas clasificaciones de virus, a continuación se presenta la clasificación de virus de acuerdo a la forma en que se ejecutan:

- Programas: archivos ejecutable con las extensiones:

[11] http://www.wikipedia.org, consultado en mayo de 2008.

.com, .exe, .drv, .ovl, .sys, .bin, .bat, etc.

También archivos con la posibilidad de ejecutar macros, como los .doc, .xls, .ppt, etc.

- Arranque: rutinas que se ejecutan durante el arranque.
- Multipartita: capaces de hacer las dos cosas anteriores.

Según la clasificación anterior, se observa que los virus pueden tener muchas modalidades o técnicas para buscar que el usuario ejecute la rutina necesaria para infectar a un host, a continuación se describen algunas de ellas:

2.6.1.1 Virus de Fichero.

Este tipo de virus se encarga de infectar programas o ficheros ejecutables (archivos con extensiones EXE o COM). Al realizar la ejecución de uno de estos programas, de forma directa o indirecta, el virus se activa produciendo los efectos dañinos que le caractericen en cada caso. La mayoría de los virus existentes son de este tipo, pudiéndose clasificar cada uno de ellos en función de su modo de actuación.

- **Virus Residentes:** Cuando se ponen en marcha, la primera acción que realizan consiste en comprobar si se cumplen todas las condiciones para atacar (fecha, hora, etc.). De no ser así, se colocan en una zona de la memoria principal, esperando que se ejecute algún programa, estos también son llamados bombas de tiempo. Si en alguna de las operaciones que realiza el sistema operativo se trabajase con un fichero ejecutable (programa) no infectado el virus lo infectará. Para ello, el virus se añadirá al programa que infecta, añadiendo su código al propio código del fichero ejecutable (programa).
- **Virus de Acción Directa:** En el momento de su ejecución, el virus trata de replicarse a sí mismo. Esto implica que creará copias de sí mismo. Cumpliéndose unas determinadas condiciones, propias en cada caso, se activará pasando a realizar infecciones dentro del directorio o carpeta en el que nos encontremos y dentro de los directorios que se encuentran especificados en la línea PATH (camino o ruta de directorios) dentro del fichero AUTOEXEC.BAT (este fichero se encuentra siempre en la raíz del disco duro, siendo un fichero de proceso por lotes que realiza ciertas operaciones cuando se enciende el ordenador). Es posible llevar a cabo la desinfección, de los ficheros afectados por el virus, dejándolos en un estado correcto.

- **Virus de Sobreescritura:** Este tipo de virus se caracteriza por no respetar la información contenida en los ficheros que infecta, haciendo que estos queden inservibles posteriormente. Aunque la desinfección es posible, no existe posibilidad de recuperar los ficheros infectados, siendo la única alternativa posible la eliminación de éstos.
- **Virus de Compañía:** Para efectuar sus operaciones de infección, los virus de compañía pueden esperar en la memoria hasta que se lleve a cabo la ejecución de algún programa (virus residentes) o actuar directamente haciendo copias de sí mismos (virus de acción directa). Al contrario que los virus de sobreescritura o los residentes, los virus de compañía no modifican los ficheros que infectan. Cuando el sistema operativo está trabajando (ejecutando programas, ficheros con extensiones EXE y COM) puede ocurrir que éste, tenga que ejecutar un programa con un nombre determinado. Si existen dos ficheros ejecutables con el mismo nombre pero con diferentes extensiones (uno con extensión EXE y otro con extensión COM), el sistema operativo ejecutará en primer lugar el que lleve la extensión COM.

  Esta peculiaridad del sistema operativo es aprovechada por los virus de compañía. En caso de existir un fichero ejecutable con un determinado nombre y extensión EXE, el virus se encargará de crear otro fichero con el mismo nombre pero con extensión COM haciéndolo invisible (oculto) al usuario para evitar levantar sospechas. Este fichero que crea será el propio virus y el sistema operativo, al encontrarse con dos ficheros que llevan el mismo nombre, ejecutará en primer lugar el de extensión COM, siendo éste el virus que en ese preciso instante realizará la infección. Tras realizarse la ejecución del fichero COM correspondiente al virus, éste devuelve el control al sistema operativo para que ejecute el fichero EXE. De esta forma el usuario no tendrá conocimiento de la infección que en ese preciso instante ha tenido lugar.

2.6.1.2 Virus de Boot

El término Boot o Boot Sector representa lo que también se denomina "sector de arranque". Se trata de una sección muy importante en un disco duro, en la cual se guarda la información sobre las características de ese disco, además de incluir un programa que permite arrancar el ordenador con ese disco, determinando

previamente si existe sistema operativo en el mismo. Este tipo de virus de Boot, no afectan a los ficheros por lo que el contenido del disco no estará en peligro a no ser que se intente arrancar el ordenador con ese disco. Si esto ocurre, el virus realizará la infección siguiendo una serie de pasos habituales:

1. Reserva un determinado espacio en memoria para que éste no sea ocupado por ningún otro programa.
2. Después de hacer esto, se coloca en esa zona reservada de la memoria.
3. Desde esa posición de memoria se encarga de interceptar servicios que realiza el sistema operativo. En cada ocasión que una aplicación del S.O. llame a una función de acceso a ficheros, el virus toma el control. De esta forma comprueba si el disco al que se accede está infectado y si no lo está, lo infecta.
4. Una última operación que realiza es volver a colocar el sector de arranque original (sin infectar), cediéndole el control, de tal forma que parezca no haber ocurrido nada. No obstante el virus seguirá actuando.
5. Las infecciones de virus de Boot se suelen realizar mediante disquetes siendo la protección contra escritura en él, el mejor método de protección.

2.6.1.3 Virus de Macro

A diferencia de los tipos de virus comentados anteriormente, los cuales infectan programas (ficheros EXE o COM) o aplicaciones, los virus de macro realizan infecciones sobre los ficheros que se han creado con determinadas aplicaciones o programas. Con ellos es posible crear documentos de texto, bases de datos, hojas de cálculo,...etc. Cada uno de estos tipos de ficheros puede tener adicionalmente unos pequeños programas, denominados macros. Una macro no es más que un micro-programa que el usuario asocia al fichero que ha creado con determinadas aplicaciones y que no depende del sistema operativo sino de acciones determinadas que el mismo usuario puede realizar dentro del documento que la contiene. Mediante ellos es posible automatizar conjuntos de operaciones para que se lleven a cabo como una sola acción del usuario de forma independiente sin necesidad de realizarlas una a una manualmente.

Estas macros son susceptibles de infección, lo que significa que los virus (más concretamente los de macro) pueden fijar sus objetivos de infección en ellas. En este caso, al abrir un documento que contenga macros, éstas se cargarán de forma automática (ejecutándose o esperando que el usuario decida ejecutarlas). En ese instante o posteriormente, el virus actuará realizando cualquier tipo de operación perjudicial. A diferencia de lo que se piensa habitualmente, los virus de macro pueden realizar acciones dañinas de bastante importancia, propagándose en poco tiempo de forma muy rápida.

2.6.1.4 Virus de enlace o de directorio

Los ficheros son los documentos que contienen la información real en la que se ha trabajado (textos, bases de datos, hojas de cálculo, imágenes, sonido,... etc.) o programas (extensiones EXE y COM) y otros tipos de "elementos" que hacen posible la ejecución de éstos. Cuando hablamos de un fichero, podemos emplear indistintamente éste término, o el de documento, o el de archivo. Para organizar toda esta información, se crean directorios o carpetas que son quienes contienen a los ficheros, pudiendo contener también otras carpetas o directorios (subcarpetas o subdirectorios). De esta forma, la estructura de un disco se puede ver como una gran carpeta clasificadora en la que los ficheros son guardados en determinadas secciones (directorios o carpetas). Otra forma diferente de presentar este concepto es pensar que el disco es una mesa de despacho en la que tenemos cajones. Estos cajones son los directorios, dentro de los cuales guardamos hojas (que representarían a los documentos, ficheros o archivos), pero que también pueden contener subsecciones (subcarpetas o subdirectorios). En definitiva el documento, fichero o archivos es el contenido y las carpetas o directorios son el continente que alberga dicho contenido.

Pues bien, el sistema informático deberá conocer en todo momento información sobre un determinado fichero, como el nombre que tiene y el lugar (carpeta o directorio) en el que se encuentra (en el que se ha guardado). Para ello le asignará una dirección a la que se debería acceder en caso de desear utilizar ese determinado fichero.

Los virus de enlace o directorio se encargan de alterar estas direcciones para provocar la infección de un determinado fichero. Si un programa (fichero EXE o

COM) se encuentra en una dirección concreta, para ejecutarlo habrá que acceder a dicha dirección. Sin embargo, el virus la habrá modificado con anterioridad. Lo que hace es alterar esta dirección para que apunte al lugar en el que se encuentra el virus, guardando en otro lugar la dirección de acceso correcta. De esta forma, cuando se pretenda ejecutar el fichero, lo que se hará realmente es ejecutar el virus.

Ya que este tipo de virus puede modificar las direcciones donde se encuentran todos los ficheros del disco, su capacidad para infectar TODOS éstos es real. De este modo, los virus de enlace o directorio pueden infectar toda la información contenida en un disco, pero les es imposible realizar infecciones en unidades de red o agregarse a los ficheros infectados. En caso de realizar un análisis del disco en busca de errores (mediante programas como SCANDISK o CHKDSK), se detectarán grandes cantidades de errores que identifican todos los enlaces a los ficheros que el virus ha modificado. No obstante, en este caso sería mejor no recuperarlos ya que podría producirse un caos en lo que al sistema de almacenamiento de la información se refiere.

El objetivo principal de los virus son los archivos que se encuentran en un medio de almacenamiento, estos ficheros afectados son archivos con características de ser programas, es decir archivos con extensiones .exe o .com. Otros virus se encargan de infectar archivos que no son programas, sin embargo estos ficheros contendrán macros incluidos en ellos. Y también están los típicos virus que atacan los archivos almacenados en discos duros.

2.6.2 Técnicas de Infección.

Existen múltiples métodos que los virus utilizan para tratar de “sobrevivir” y ejecutarse en el mundo de las redes, entre las diversas técnicas que los virus utilizan tenemos:

- **Ocultamiento (Stealth):** Los virus que utilizan esta técnica intentan pasar desapercibidos ante los ojos del usuario, no levantando ninguna sospecha sobre la infección que ya ha tenido lugar. Los virus residentes son los que más la utilizan, aunque no es exclusivamente este tipo de virus quienes la aplican.
  Cuando un virus infecta un determinado fichero, suele dejar signos evidentes de su actuación, como los siguientes: aumento de tamaño en el fichero infectado, modificación de la fecha y hora de creación en el fichero infectado, secciones marcadas como defectuosas, disminución de la capacidad en la memoria, etc. El

virus se encargará de que cada una de estas pistas no puedan ser visualizadas. Para ello vigilará peticiones de información que requiere el sistema operativo acerca de estas características, interceptándolas y ofreciendo una información falsa.

- **Sobrepasamiento (Tunneling):** Se trata de una técnica especialmente diseñada para imposibilitar la protección antivirus en cualquier momento. Mientras el análisis permanente, o residente, del programa antivirus que se encuentre instalado intenta realizar detecciones, el virus actúa en su contra. Todas las operaciones que se realizan sobre cualquiera de los archivos son inspeccionadas por el antivirus mediante la interceptación de las acciones que el sistema operativo lleva a cabo para hacerlas posible. De la misma manera, el virus interceptará estas peticiones o servicios del sistema operativo, obteniendo las direcciones de memoria en las que se encuentran. Así el antivirus no detectará la presencia del virus. No obstante, existen técnicas antivirus alternativas que permiten la detección de virus que realicen este tipo de operaciones.

- **Autoencriptación:** Los programas antivirus se encargan de buscar determinadas cadenas de caracteres (lo que se denomina la firma del virus) propias de cada uno de los posibles virus. Estos, por su parte y mediante la técnica de autoencriptación, infectarán de forma diferente en cada ocasión. Esto significa que el virus utilizará una cadena concreta para realizar una infección, mientras que en la siguiente infección utilizará otra distinta. Por otro lado, el virus codifica o cifra sus cadenas para que al antivirus le sea difícil encontrarlo. Sin embargo, los virus que utilizan este tipo de técnicas, emplean siempre la misma rutina o algoritmo de encriptación, con lo que es posible su detección.

- **Polimorfismo:** Basándose en la técnica de autoencriptación, el virus se codifica o cifra de manera diferente en cada infección que realiza (su firma variará de una infección a otra). Si sólo fuese así estaríamos hablando de un virus que utiliza la encriptación, pero adicionalmente el virus cifrará también el modo (rutina o algoritmo) mediante el cual realiza el cifrado de su firma. Todo esto hace posible que el virus cree ejemplares de sí mismo diferentes de una infección a la siguiente, cambiando de "forma" en cada una de ellas. Para su detección, los programas antivirus emplean técnicas de simulación de descifrado.

- **Armouring:** Mediante esta técnica el virus impide ser examinado. Para conocer más datos sobre cada uno de ellos, éstos son abiertos como ficheros que son, utilizando programas especiales (Debugger) que permiten descubrir cada una de las líneas del código (lenguaje de programación en el que están escritos). Pues bien, en un virus que utilice la técnica de Armouring no se podrá leer el código.

Otros términos que se comúnmente se encuentran ligados a los virus, se mencionan a continuación:

Troyano: no es directamente un virus, dado que no se reproduce. Son programas ejecutables que son ingresados a un sistema por un usuario malicioso de forma encubierta, como un programa amistoso, gráficos, juegos, etc. De esta manera, al ser ejecutados, realizan acciones que el usuario no desea y que fueron desarrolladas por el escritor troyano.

Gusano: son programas que tratan de reproducirse a sí mismo, no produciendo efectos destructivos sino el fin de dicho programa es el de colapsar el sistema o ancho de banda, replicándose a sí mismo o reenviándose a gran cantidad de usuarios a través de una red.

2.6.3 Antivirus

Un antivirus es un programa capaz de detectar virus dentro del sistema y desinfectarlo. Existen varios métodos que utilizan los antivirus para detectar virus informáticos:

- **Búsqueda de cadenas**
  Cada uno de los virus contiene determinadas cadenas de caracteres que le identifican. Estas son las denominadas firmas del virus. Los programas antivirus incorporan un archivo denominado "fichero de firmas de virus" en el que guardan todas las cadenas correspondientes a cada uno de los virus que detecta. De esta forma, para encontrarlos, se analizarán todos los archivos especificados comprobando si alguno de ellos las contiene. Si un fichero no contiene ninguna de estas cadenas, se considera limpio, mientras que si el programa antivirus la detecta en el interior del archivo avisará acerca de la posibilidad de que éste se encuentre infectado.

- **Excepciones**

  Una alternativa a la búsqueda de cadenas es la búsqueda de excepciones. Cuando un virus utiliza una determinada cadena para realizar una infección pero en la siguiente emplea otra distinta, es difícil detectarlo mediante la búsqueda de cadenas. En ese caso lo que el programa antivirus consigue es realizar la búsqueda concreta de un determinado virus.

- **Análisis heurístico**

  Cuando no existe información que permita la detección de un nuevo o posible virus desconocido, se utiliza esta técnica. Se caracteriza por analizar los ficheros obteniendo información sobre cada uno de ellos (tamaño, fecha y hora de creación, posibilidad de colocarse en memoria, etc.). Esta información es contrastada por el programa antivirus, quien decide si puede tratarse de un virus, o no. Entre las diversas técnicas heurísticas utilizadas se tienen: firmas genéricas, reconocimiento del código compilado, desensamblado, desempaquetamiento.

  Firmas genéricas: los virus son modificados constantemente a fin de no ser detectados, estas variaciones generalmente contienen similitudes con los códigos originales lo cual se denomina una familia de virus, los antivirus heurísticos pueden reconocer a toda la familia en base a similitudes en el código fuente, permitiendo así, la detección de amenazas sin necesidad de actualización.

  Código compilado: cuando un programa es compilado para convertirlo en archivo ejecutable, la codificación resultante representa instrucciones que se le darán al sistema para efectuar ciertas acciones. Esta técnica identifica las instrucciones comúnmente aplicadas por los códigos maliciosos para identificar si pudiera o no considerarse como amenaza.

  Desensamblado: todo archivo ejecutable puede ser desensamblado con el objetivo de obtener el código fuente del programa en lenguaje ensamblador; esta técnica es capaz de analizar el código fuente de los programas sospechosos con el fin de reconocer en el técnicas de desarrollo que sean usadas por programadores de virus y así reconocer un código malicioso nuevo.

  Desempaquetamiento: los programadores de códigos maliciosos suelen usar empaquetadores de archivos con el fin de modificar la apariencia del virus a los ojos del análisis antivirus. Empaquetadores son usados para esto, pero para evitar ser engañado el antivirus analiza el código real del programa y no el empaquetado.

- **Protección permanente**
  Durante todo el tiempo que el dispositivo permanezca encendido con las licencias activas, el aplicativo de antivirus se encargará de analizar todos los ficheros implicados en las operaciones diarias. Cuando los archivos se copian, se abren, se cierran, se ejecutan, etc., es decir se genera algún tipo de actividad que involucre el paso del archivo por el dispositivo él antivirus los analiza. En caso de haberse detectado un virus se muestra un aviso en el que se permiten la desinfección o se le informa al administrador de lo encontrado. Si no se encuentra nada extraño, el proceso recién analizado continúa.

2.7 IM & P2P.

Se tratan ambos temas a la vez ya que las técnicas para comunicarse y controlar estas aplicaciones son similares, se iniciara por definir los conceptos básicos de cada una de ellas, explicar su funcionamiento y posteriormente los métodos usados para la identificación de este tipo de aplicaciones.

2.7.1 P2P

Se le llama P2P (peer-to-peer o de punto a punto) a una red que no tiene clientes ni servidores fijos, sino una serie de hosts que pueden funcionar como clientes o servidores de los demás host de la red, estas redes se conforman de forma lógica usando la infraestructura técnica de Internet pero basándose en la búsqueda del recurso en base a su descripción no importando la ubicación o en el host en el cual se encuentre. Estas redes en las cuales los mismos host desempeñan funciones de servidores y clientes se les llamas redes ad-hoc[12].

En un principio P2P significaba una comunicación de igual a igual entre dos dispositivos, sin embargo para esto habría que contar con una infraestructura completa para proporcionar la comunicación de igual a igual entre dos host, por lo anterior hoy en día se maneja el concepto de P2P de manera lógica estableciendo circuitos virtuales entre host, los cuales ya no cumplen la función de ser simples PC’s sino que ahora son llamados nodos que pueden funcionar como clientes o servidores dependiendo de la necesidad o los recursos solicitados.

[12] Documento consultado Peer-to-Peer, Escuela de Castellanos

Los P2P son redes que aprovechan, administran y optimizan el uso del ancho de banda que acumulan de los demás usuarios en una red por medio de la conectividad entre los mismos usuarios participantes de la red, siendo estas capaces de utilizar todo el ancho de banda disponibles por los usuarios, obteniendo así un mayor rendimiento en las conexiones y transferencias que con los métodos centralizados donde una cantidad relativamente pequeña de servidores provee el total ancho de banda y recursos compartidos para un servicio o aplicación.

2.7.1.1 Configuraciones lógicas de redes P2P

Estas redes P2P se utilizan comúnmente para compartir toda clase de archivos ya sea de audio, video, texto, software o datos en cualquier formato digital. Las configuraciones de redes P2P también tienen sus variaciones, entre las más comunes tenemos:

- ***Redes centralizadas***
  Este tipo de red se basa en una arquitectura monolítica de un solo servidor central el cual es la interconexión de todos los host, resultando por tanto con limitaciones de ancho de banda hacia todos los host, falta de escalabilidad, falta de privacidad de los usuarios, problemas de puntos de fallo. Ejemplos de aplicaciones que utilizan este modelo Napster y Audiogalaxy.

- ***Redes descentralizadas***
  *S*on las más comunes, permitiendo la versatilidad de no depender de un solo equipo de hecho no existe el servidor central, optando por que sean los propios usuarios los servidores o clientes dependiendo de la necesidad y estos se enlazan por nodos que a su vez están compuestos por más usuarios. Ejemplo de aplicaciones que utilizan este modelo: Ares, KazaA, Gnutella, Gnutella 2.

- ***Redes hibridas***
  Aquí existe la interacción de un servidor central quien administra los recursos y la comunicación entre nodos, que a su vez pueden ser más servidores o los mismos clientes, teniendo la peculiaridad que si los servidores caen la comunicación podrá mantenerse activa entre todos los host, con un modelo como el antes mencionado. Ejemplo de aplicaciones que utilizan este modelo: Bittorrent, EDonkey2000, Emule.

En la figura 2.10 se presenta una ilustración de las configuraciones lógicas de una red P2P

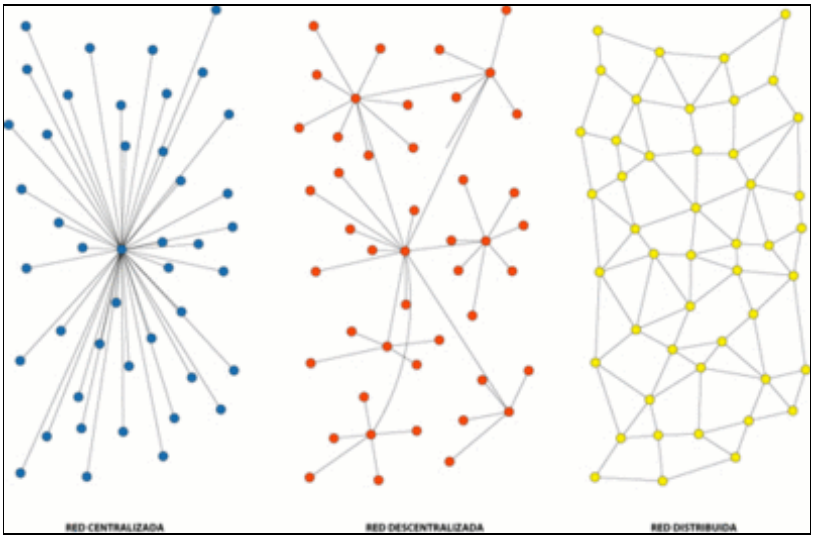


Figura 2.10 Diagramas lógicos de redes P2P.

2.7.1.2 Generaciones de P2P

La primera aplicación P2P fue desarrollada en 1996 para el sistema operativo Mac OS su nombre fue: Hotline Connect, la cual pretendía ser una plataforma de distribución de archivos destinada a empresas y universidades de manera descentralizada, pero no tardo en servir todo tipo de archivos sobre todo de pornografía; sin embargo por tratarse de una aplicación desarrollada para una plataforma minoritaria (Mac OS) no causo ningún efecto en el mundo de la informática.

a) *Primera Generación*

   En un inicio, estaba basado sobre servidores centralizados, estos actuaban como árbitros de todo lo que sucedía en la red, se encargaban de las conexiones entre los host involucrados, sin embargo debido al uso excesivo de servidores, este tipo de redes resulto inestable y poco confiable, y su propia estructura facilitaba acumular la información que se transmitía entre los clientes lo que posteriormente fue usado para acusar por demandas en contra de los derechos de autor.

Su sistema más representativo fue Napster el cual inicio en 1999, atribuyéndosele a este la creación de aplicaciones P2P; aunque en realidad las transferencias de los archivos tenían lugar directamente entre dos equipos, Napster y Audiogalaxy usaban servidores centrales para almacenar la lista de equipos y los archivos que proporcionaba cada uno por lo que no era una aplicación propia de P2P como la conocemos actualmente.

Napster se presento como la primera aplicación para PC que podía transferir archivos de música mp3, lo que causo el rotundo éxito y posteriormente su cierre por problemas legales al ser demandado por derechos de autor en el año 2001 para ese entonces ya contaba con 13.6 millones de usuarios[13].

a) Segunda Generación

Luego de lo observado y del cierre de varias aplicaciones P2P de primera generación, se reorganizó la estructura de estas aplicaciones. Se definió suprimir en su totalidad el sistema centralizado de servidores, pasando a una nueva estructura en donde se tenían a los host como posibles clientes o servidores, dependiendo de la necesidad, llamándoles a estos nodos.

Posteriormente se desarrollaron los supernodos, que son nodos con mayor importancia por contar con más capacidad de información y retransmisión, los cuales sin llegar a ser servidores tienen una capacidad superior a los simples nodos. Lográndose con lo anterior una optimización de los recursos que pudo ser observado en las altas tasas de transferencia que son sin duda una de las claves del éxito de estas aplicaciones.

Fue por esto que en el año 2002 se dio un éxodo masivo a las aplicaciones descentralizadas, que ya no presentan la facilidad de llevar un registro de los archivos transferidos en un solo servidor, de la misma manera ya era posible el intercambio no solo de música sino también de todo tipo de archivos. En la figura 2.11 se presentan logos de aplicaciones P2P de primera y segunda generación respectivamente.

Es importante aclarar que una aplicación P2P que muchas veces no se considera como tal pero que se tomara en cuenta en este trabajo es la aplicación de Skype, la

[13] http://www.wikipedia.org, fecha de consulta: mayo de 2008

cual si bien es cierto tiene muchas semejanzas a simple vista con aplicaciones IM, por la forma de su estructura y las características técnicas de la misma, se considera como una aplicación P2P más, de igual manera no todos los fabricantes lo incluyen en las funcionalidades de sus equipos.

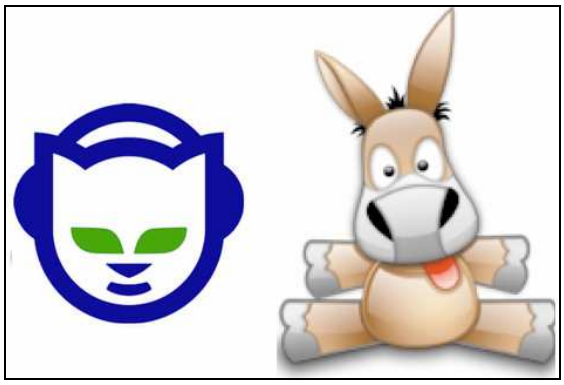


Figura 2.11 Imágenes representativas de aplicaciones P2P de primera y segunda generación, Napster y Emule respectivamente.

Hoy en día según datos proporcionados por Sandvine un prestigioso fabricante de equipos administradores de ancho de banda, se calcula que el porcentaje de tráfico generado por aplicaciones P2P es alrededor del 70 % del total de tráfico circulante en Internet. Por otro lado la configuración más usada por las actuales aplicaciones P2P es la de redes mixtas.

b) Tercera generación

En la actualidad ya está en implementación la tercera generación de las aplicaciones P2P, esta tiene como características ofrecer una mayor seguridad en el tipo de archivos transferidos, así como contar con unas mayores tasas de transferencia a las existentes hoy en día, sin embargo el mayor cambio que se vislumbra es la implementación de redes P2P puras y funcionales entre los clientes de estas aplicaciones.

Si lo anterior llegase a cumplirse, se podría predecir la extinción de los servidores principalmente porque para esta implementación requerirá de maquinas con grandes recursos de procesamiento y anchos de banda no tan comunes en nuestros días en los host de cada cliente; a esto cabe mencionar que también se está trabajando para que esta nueva generación no permita conocer la identidad de los clientes que usan la aplicación esto se realiza encriptando la IP de los usuarios. En la actualidad está

en periodo de prueba (comúnmente llamada versión Beta) la aplicación P2P de tercera generación llamada MUTE, en la figura 2.12 se presenta una ilustración de ella.

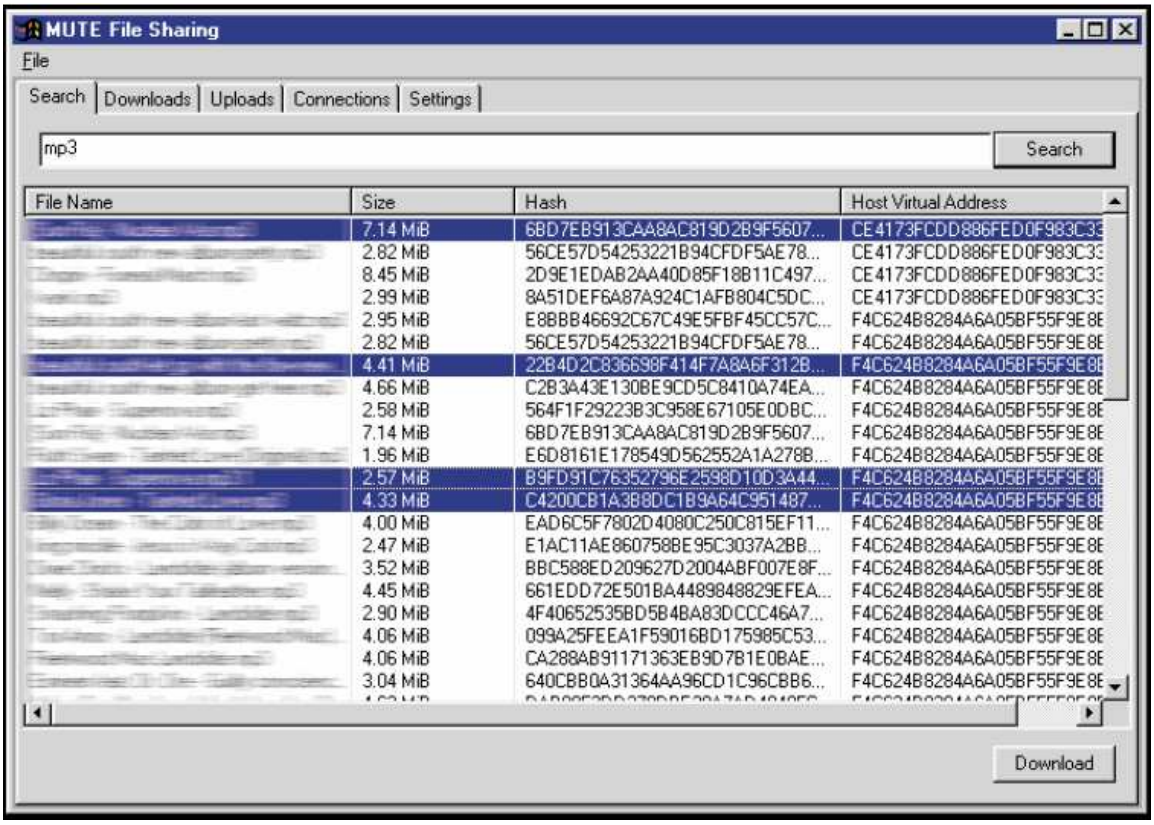


Figura 2.12 Ilustración de MUTE aplicación de P2P de tercera generación.

2.7.2 IM

Desde el nacimiento de internet, los sistemas de mensajería instantánea se han convertido en un medio de comunicación masivo y eficaz para cualquier usuario debido a la simplicidad y rapidez de su manejo, constituyendo en la actualidad la vía de comunicación preferida para entablar una conversación en tiempo real. Por lo antes mencionado, también se ha convertido en una fuente altamente explotable para la difusión y diseminación de códigos maliciosos de todo tipo, resultando que la mensajería instantánea sea un medio muy utilizado para este fin.

La mensajería instantánea realiza las conversaciones en tiempo real, permitiendo además el intercambio de todo tipo de archivos, además de extras como videoconferencias, llamadas telefónicas a cualquier parte del mundo solo basta con tener el mismo cliente que la contraparte y estar conectado en el mismo momento, aunque también en la actualidad se pueden dejar mensajes a usuarios que se encuentren offline.

El IM (Instant Messenger) que se conoce en la actualidad tiene sus orígenes en un sistema generalizado de asistencia computacional creado en la década de los setentas denominado PLATO (Programed Logic Automated Teaching Operations). A partir de allí fueron desarrollándose otras aplicaciones, tales como Talk en el año 1990 e implementado para sistemas UNIX/LINUX, el ICQ creado durante el año 1996 y disponible tanto para sistemas UNIX/LINUX como para Windows[14].

Desde entonces, muchas aplicaciones fueron surgiendo hasta llegar a las que se conoce actualmente, incluso combinando diferentes servicios como VoIP, videoconferencia, etc. Las aplicaciones más comunes y utilizadas son AOL Messenger, Yahoo Messenger, MSN Messenger y Google Talk, es de aclarar que cada una de estas necesita su propio cliente para poder usarse aunque recientemente es posible usar cuentas de otros servidores para usarse en los clientes que se desee, sobre todo con las aplicaciones de protocolo abierto como google talk que utiliza el protocolo Jabber[15].

3.7.2.1 Funcionamiento IM

El servicio de mensajería instantánea en un inicio se basaba en una estructura propiamente de cliente-servidor, en donde varios servidores se interconectan entre sí teniendo cada uno a muchos más clientes pegados a estos y permitiendo que los clientes de todos los servidores pudieran comunicarse entre ellos. Los servidores usaban diagramas de árbol que les permitían conocer un solo camino de comunicación (también conocido como spanning tree) hacia cada usuario, al mismo tiempo eran capaces de conmutar las rutas en caso de fallo de alguna ruta existente.

[14] http://www.wikipedia.org, consultado en mayo de 2008
[15] JAbber: protocolo libe para mensajería instantánea.

En la actualidad, el servicio de mensajería instantánea se basa en el SIP (Session Initiation Protocol), el cual se origino a mediados de los años noventas siendo un proceso de señalización para establecer llamadas o conferencias en redes IP, convirtiéndose con el tiempo en estándar de comunicaciones o aplicaciones que requieran presencia de usuarios.

SIP es el encargado de regir la manera en como conocemos hoy en día la mensajería instantánea, entre las principales características de esta aplicación tenemos:

- Velocidad de comunicaciones: que permiten ubicar, enlazar e intercambiar datos en usuarios tan rápido que pareciera en tiempo real.
- Dinamicidad de ubicación del usuario, dando la facilidad de comunicar a los usuarios desde cualquier parte que estos inicien sesión sin importar la distancia, la clase de equipo usado (PC, teléfono celular, PDA, etc.) o el sistema operativo de los mismos.
- Transporte de información: la misma velocidad requerida por la aplicación obliga a los clientes a enviar mensajes de simple estructura basados en códigos ASCII de una sola línea, los clientes realizan peticiones pero sin importar si estas son respondidas o no por los servidores u otros usuarios.
- Registro de usuarios: la identidad o cuenta de cada usuario (ej.: nombre@yahoo.com) es única e irrepetible por cada gestor de mensajería, facilitando la movilidad del mismo aquí se restringen los caracteres alfanuméricos que la conforman; por otro lado el nombre personalizado (ej.: Juan, C4rl0s, etc.) que el usuario puede contener no tiene restricciones de caracteres y puede ser similar entre varios usuarios.

El funcionamiento del servicio de IM requiere:

- *Cliente de Messenger:* son los procesos que se ejecutan en el equipo del usuario de la aplicación una vez han sido correctamente instalados (ej.: Msnmsgr.exe, Yahoo Mesenger, aMSN). Estas realizan las funciones básicas de IM así como las tareas de integración de servicios, programas y/o aplicaciones (mail, netmeeting, multimedia, etc.)
- *Dispatch Server (DS)*: es el punto inicial de conexión entre el cliente y el IM. Sus funciones principales son la determinación de que Notification Server (NS) está asociado con el cliente destino, es decir con el que se quiere hacer la conexión vía algoritmo a elección del servidor y la redirección del cliente al NS apropiado.
- *Notification Server:* es el componente servidor primario, el cliente y el NS se autentican, sincronizan las propiedades del usuario e intercambian notificaciones de

eventos asíncronas. La conexión del cliente al NS ocurre cuando la redirección desde el DS ha terminado y persiste sin interrupción durante la sesión del usuario en el IM. Algunos de los eventos transmitidos entre un cliente y un NS son: cambios de estado del cliente (online, offline, idle, etc.), peticiones de invitación o aplicaciones especificas como nuevo mensaje de correo o invitación a videoconferencia.

- *Switchboard Server (SB):* es el componente a través del cual los clientes pueden establecer sesiones de comunicación ligeras es decir, sin requerir una conexión directa entre clientes. Por lo que podríamos decir que el uso habitual del SB es proveer sesiones de IM. Así, cuando un cliente desea comunicarse con otro cliente, envía un mensaje a su NS, el cual redirige a un SB. Una vez la conexión con el SB se ha establecido, el cliente destino recibe una notificación desde su NS para conectarse al mismo SB.

En la figura 2.13 se observa una representación de los elementos antes mencionados.

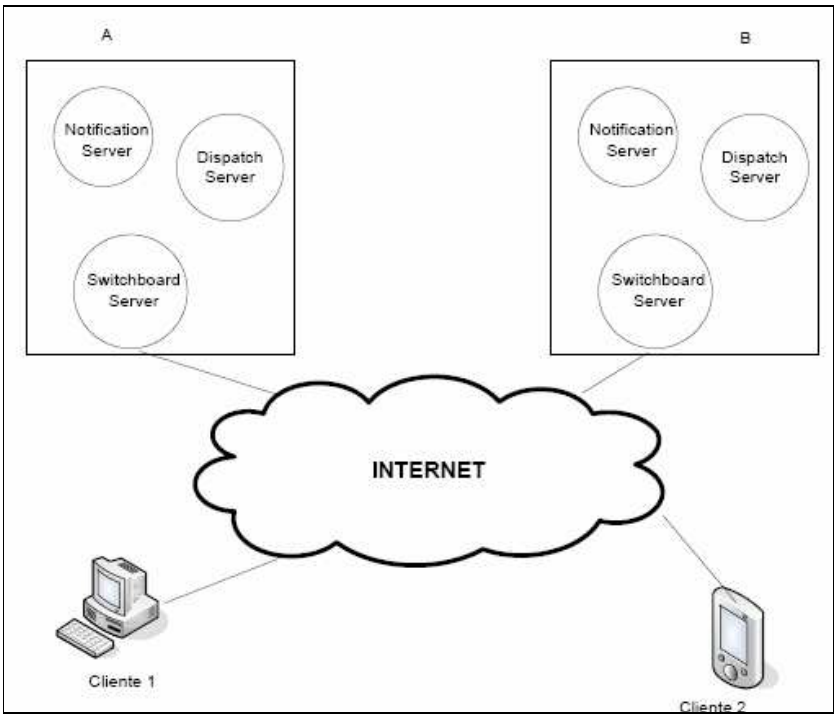


Figura 2.13 Ilustración de los elementos del IM

2.7.3 Métodos para identificar protocolos

Como se ha observado anteriormente, algunos protocolos pueden ser identificados o bloqueados por el número de puerto, sin embargo para este tipo de aplicaciones en especial (P2P e IM) lo anterior no aplica ya que estas son denominadas “aplicaciones inteligentes”, por los motivos explicados en el párrafo siguiente.

Estas aplicaciones tienen la característica que si se llegase a bloquear puertos que estos comúnmente usan para comunicarse, estas aplicaciones son capaces de buscar puertos abiertos en los host y comunicarse por estos otros, como medida extrema son capaces de comunicarse por puertos usados para aplicaciones comunes como el puerto 25 usado para correo, el puerto 23 usado para telnet, el puerto 21 usado para FTP, o incluso el puerto 80 es decir el de HTTP, haciendo prácticamente imposible el bloqueo de estas aplicaciones por esta técnica ya que de bloquearse este último puerto se estaría restringiendo todas las aplicaciones web.

Sin embargo existen otras más que si son utilizadas para restringir o bloquear estas aplicaciones, entre estas tenemos:

2.7.3.1 Técnica heurística

Evalúa las conexiones de las aplicaciones que generalmente se conectan al mismo server o grupos de servers en internet antes de completar todos los intercambios requeridos para iniciar la aplicación, por ejemplo las aplicaciones de IM se conectan a un servidor central de IM para conseguir código de acceso y generar la información de su presencia en la red. Esto permite identificar con cierto grado de certeza el tipo de aplicación que se intenta iniciar al determinar el tipo de servidor al que se está intentando conectar. Similar panorama se presenta para trafico P2P en donde los servidores remotos tienden a ser los mismos y se conectan en un inicio mediante puertos ya establecidos o definidos por algunos de ellos; sin embargo algunas aplicaciones siempre se conectan mediante puertos aleatorios, al encontrarse bloqueados los puertos usados comúnmente.

En la tabla 2.3 Se presenta un listado de las aplicaciones más usadas y los respectivos puertos asociados a cada una.

Aplicación	Puerto	Protocolo
Linmewire	6346 / 6347	TCP / UDP
Edonkey	4662	TCP
EMule	4662 / 4672	TCP / UDP
Bittorrent	6881 - 6889	TCP / UDP
KaZaa	1214	TCP
Gnutella	6346 - 6347	TCP / UDP
Skype	80 / 443	TCP
IM	5160 - 5190	TCP
AOL	1863	TCP
YMSG	5050	TCP

Tabla 2.3 Aplicaciones más usadas con sus respectivos puertos por defecto.

2.7.3.2 Patrones

Método poco utilizado pero considerado un tanto efectivo, su técnica consiste en determinar patrones de trafico es decir comportamiento típico de cada aplicación para así lograr identificar la naturaleza del mismo. Sin embargo este tiene ciertas limitantes, únicamente funciona con aplicaciones P2P con estructura descentralizada y estas mismas aplicaciones deben de basar su negociación en protocolo UDP para obtener óptimos resultados en su análisis. En la tabla 2.4 se presenta una descripción de ciertas aplicaciones P2P que pueden ser identificadas con esta técnica, según lo muestra securityfocus en su página web.

Aplicación	Patron
Edonkey	Usa paquetes UDP de 6 bytes para enviar el resquest de estato del servidor. El paquete de desempeño de busqueda tiene longuitud de 25 bytes
Limeware	Utiliza paquetes UDP de 23 y 35 bytes de request a los clientes cuando este se esta iniciando; ademas cada vez que inicia una descarga el tamaño de la paqueteria es de 23 Bytes UDP.
Skype	Desde su inicio utiliza paquetes de longuitud de 18 bytes UDP para comunicarse con sus clientes.
Kazaa	Envia continuamente paquetes UDP de 12 bytes de longuitud hacia los detinatarios
Emule	Al seleccionar el server a usar se envian paquetes de 6 bytes, luego de esto el envio de paquetes es continuo y varia entre 27 y 35 Bytes UDP.
Gnutella	Se envian paquetes de 19 bytes UDP durante todo el tiempo que esta levantada la aplicación.

Tabla 2.4 Patrones de aplicaciones P2P

2.7.3.3 Firmas

Esta es la técnica más usada para identificar estos protocolos, las firmas son "huellas" que describen un patrón de paquetes en la red, estos patrones identifican con certeza a protocolos específicos debido a que este patrón es único para cada tipo de tráfico, por lo anterior se le considera un método con alto grado de certeza.

Las firmas de las tramas se examinan en la capa 7 o capa de aplicación, esto debido a que en la sección de payload o datos es donde se oculta o se determinan las firmas requeridas. En la tabla 2.5 se muestra una imagen con los caracteres que se pueden encontrar en las firmas de algunas aplicaciones P2P.

P2P Protocol	*String*	*Trans. prot.*	*Def. ports*
eDonkey2000	0xe319010000	TCP/UDP	4661-4665
	0xc53f010000		
Fasttrack	"Get /.hash"	TCP	1214
	0x270000002980	UDP	
BitTorrent	"0x13Bit"	TCP	6881-6889
Gnutella	"GNUT", "GIV"	TCP	6346-6347
	"GND"	UDP	
MP2P	GO!!, MD5, SIZ0x20	TCP	41170 UDP
Direct Connect	"$MyN","$Dir"	TCP	411-412
	"$SR"	UDP	
Ares	"GET hash:"	TCP	-
	"Get sha1:"		

Tabla 2.5 Cadenas de caracteres encontradas en trafico P2P, usadas para definir firmas[16]

Los métodos de identificación pueden como se describe en la figura anterior, determinarse en base a los caracteres iniciales "0x" de cadenas que son comunes entre algunas aplicaciones P2P, además se puede utilizar los puertos iníciales y/o finales para determinar el tipo de aplicación solicitada, o simplemente evaluar el paquete de datos y verificar el encapsulado de capa de transporte.

Muchas veces es necesario valerse además de la firma de cada aplicación de puertos usados o cadenas de caracteres, para no generar falsos positivos. En la tabla 2.6 se muestra el listado de firmas para algunas aplicaciones comunes definidas para P2P e IM.

Aplicación	**Firma**
MSN Messenger	MSN Messenger
Windows Messenger	MSMSGS
AOL Messenger	Gecko/
Yahoo Messenger	YSMG
Kazaa	KaZaA o Kazaa
Gnutella	Gnutella o Gnucleus
Edonkey	e2dk
Emule	e2dk
BitTorrent	BitTorrent
Skype	Skype

Tabla 2.6 Firmas definidas para algunas aplicaciones comunes de P2P e IM[17]

[16] University of Calgary, consultado en mayo de 2008
[17] http://www.microsoft.com, consultado en mayo de 2008

2.8 Reportes.

Un punto de mucha importancia de los UTM es la capacidad de almacenar logs del tráfico, tomando en cuenta que todo el tráfico de la red es enrutado y analizado por estos dispositivos, se nos hace fácil pensar que de una u otra forma se tiene un control de cada usuario y aplicación en todo momento. Lo anterior toma una mayor importancia cuando se presenta la posibilidad de generar algún tipo de registro o reporte del desempeño que ha tenido el equipo en un tiempo determinado. Si bien es cierto la capacidad de generar reporte no necesariamente viene incluida en todo dispositivo, si es un agregado que muchos fabricantes han tomado en cuenta para ofrecerlo a sus usuarios.

Estos logs también ofrecen la capacidad de anexarse a aplicaciones que suelen usarse para registrar los eventos de la red en general como por ejemplo syslogs o servers destinados a este fin; incluso algunos fabricantes crean dispositivos específicos para almacenar todos los logs para así generar reportes de una mayor calidad y flexibilidad que los que almacenan todos los eventos en el mismo dispositivos o en una PC de la red. Sin embargo estos últimos representan un mayor costo monetario para el usuario final.

Los elementos con los que cuenta de manera general los reportes, son los que comúnmente interesan a los administradores de red para determinar el desempeño de la red o si en dado caso existiese saturación o alguna anomalía en la red esta pudiera ser registrada con facilidad. Entre los principales puntos de importancia se tiene la utilización del ancho de banda por horas del día, la clase de aplicaciones que los usuarios utilizan comúnmente, las posibles anomalías que se estuvieran generando desde la LAN hacia afuera, sin embargo estos reportes pueden llegar a ser un tanto limitados por el solo hecho de estar incluido en el UTM sobretodo en el aspecto del almacenamiento de información que se pudiera dar en el mismo dispositivo o en equipos del cliente. En la figura 2.14 se presenta una muestra de reporte incluido en un dispositivo.

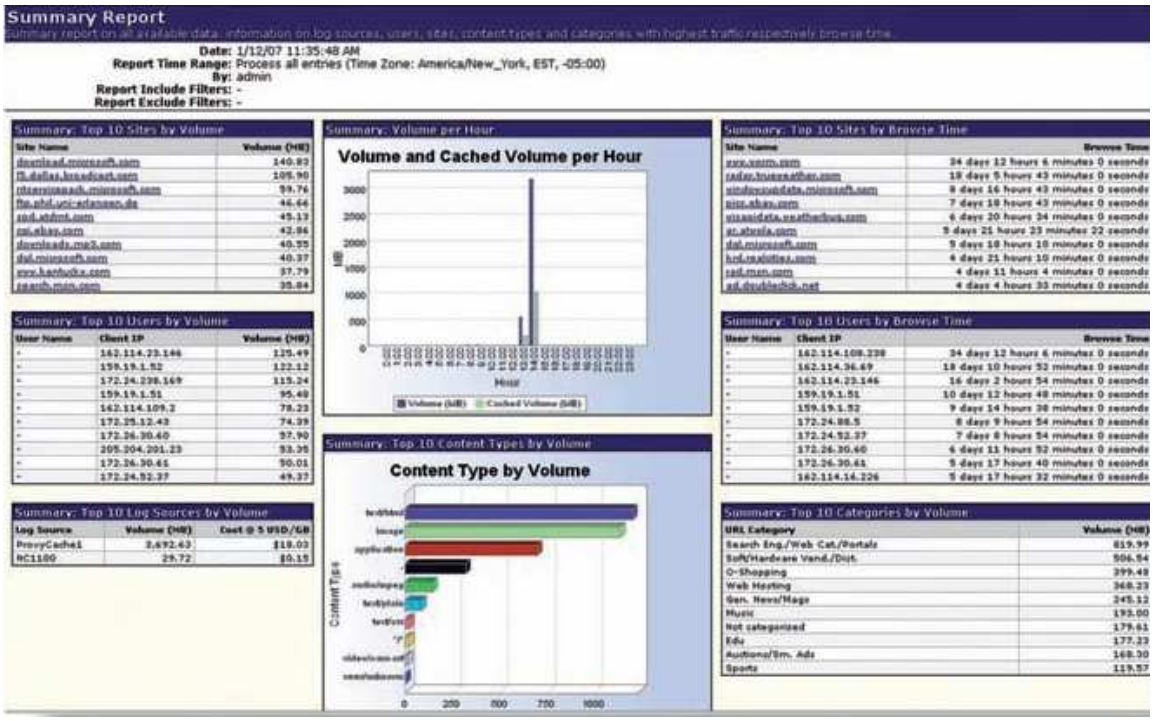


Figura 2.14 Imagen de un UTM que incluye el segmento de reportes.

De la misma manera, existen clientes (generalmente bancos o financieras) que demandan conocer toda la información de correo, Messenger, etc. que se ha transferido desde los host de la empresa, ya sea hacia afuera o hacia la misma LAN por la misma naturaleza de la información que se maneja, esto es posible en la mayoría de los casos con la ayuda de dispositivos o aplicaciones externas; que a su vez facilitan el filtro de información para mostrar únicamente la información requerida.

Estas estadísticas se presentan en forma de gráficos y tablas para hacerlos un tanto más comprensibles para el usuario, estas graficas están incluidas en extensos documentos formales, generalmente en formato pdf donde se muestra con detalles las eventos registrados por usuario, grupos de usuarios, protocolos, visitas a sitios web, horas del día, etc. En la figura 2.15 se muestran imágenes de un dispositivo externo diseñado únicamente para registrar logs y generar reportes al conectarse al UTM principal.

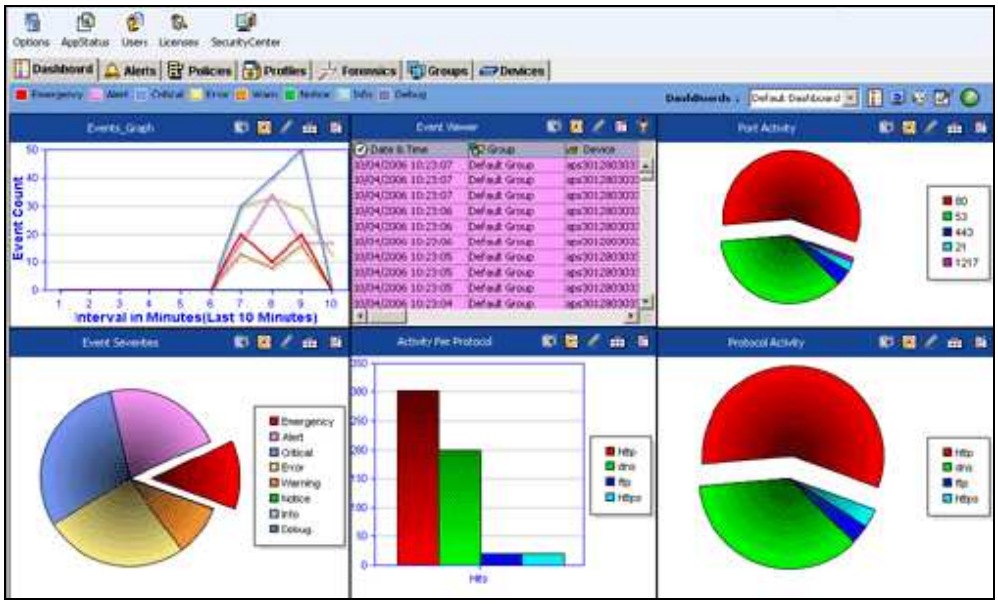


Figura 2.15 Imágenes de dispositivo diseñado para almacenar logs y generar reportes

2.9 Áreas no cubiertas

Los UTM son dispositivos de seguridad periférica, lo que nos indica que este identificara y enlutara el tráfico entre al menos dos interfaces que estén directamente conectados a este. Es decir se tendrá control del tráfico entre la comunicación de las redes que utilicen como "pasarela" al dispositivo, sin embargo no es un dispositivo de usuario final que pudiese regular o detectar las amenazas que son generadas desde dentro de la LAN.

Por ejemplo si se tuviese un usuario con algún virus, malware o spyaware en dispositivos externos como CD, DVD, memoria SD, dispositivos USB, etc. y se llegase a infectar al host, el dispositivo no funcionará como antivirus o antispyware para el host ya que la anomalía se genero desde dentro de la LAN, simplemente este funcionara como limitador de tráfico, impidiendo que la red interna pudiese estar propagando anomalías a la red externa y registrando el segmento o host interno infectado.

Se requiere de una conexión permanente a Internet con licencias validas de actualización, lo anterior es de vital importancia si se quiere contar con las últimas protecciones desarrolladas ante las amenazas más recientes; ya que en su totalidad estos dispositivos se están actualizando periódicamente para estar al día con la protección periférica. El mismo

panorama se presenta para la categorización de páginas web y el control de tráfico, ya que los registros e identificación de tráfico se realizan mediante consultas a servidores ubicados en diversas partes del mundo que requieren tener licencia válida para proveer de sus servicios.

La utilidad de cache que algunos firewalls montados en software o servidores proxy otorgan, en muchos casos no son ofrecidos por varios fabricantes de estos dispositivos, esto debido a que la memoria con la que cuentan los UTM muchas veces es demandada por otras aplicaciones y estos equipos no son diseñados específicamente para esta actividad. Sobre todo porque la categorización de las páginas es accesada cada cierto tiempo para asegurar que esta no contenga información restringida o haya sido víctima de algún ataque que pudiera perjudicar a los usuarios finales.

Los dispositivos UTM como hemos visto, necesitan estar actualizando sus bases de datos continuamente, esto lo realizan en base a licencias que cada fabricante determina, estas sin embargo están limitadas a cierto tiempo de utilidad, por lo que es necesario estar renovando el servicio continuamente sumándole a esto que si se adquiere un dispositivo existe la posibilidad que para el siguiente año o dos años el modelo sea anticuado para los fabricantes y opten por no sacar actualizaciones para ese modelo, por lo que debe de existir coherencia entre el hardware adquirido y las actualizaciones posibles a los siguientes por lo menos cinco años.

Capitulo 3: Introducción

En el siguiente capítulo se presenta una descripción de las principales aplicaciones que son posibles realizar en los dispositivos UTM, sin embargo estas pueden variar de fabricante en fabricante o de modelo en modelo, pero se ha presentado las más importantes de estas enfocando las principales características y necesidades que estas pueden llegar a solventar en un ambiente real.

Se han separado en cinco apartados dependiendo del área que estas cubran, para mostrar los beneficios en cada área en específico. Las categorizaciones utilizadas son:

- Controlar trafico de la red
- Regular acceso de los usuarios a Internet
- Sistemas de seguridad en la red
- Creacion de VPN confiables
- Complementos

3.0 UTILIDAD DE DISPOSITIVOS UTM

Figura 3.1 Ilustración de aplicaciones en los UTM

3.1 Controlar tráfico en la red

Los dispositivos UTM como se ha presentado en el capítulo anterior, tienen diferentes herramientas orientadas al servicio de un buen desempeño de la red de trabajo, entre las protecciones que este equipo proporciona se incluyen:

- Anti-Spyware
- Antiphising
- Control de aplicaciones Instant Messenger (IM) / P2P
- Control de aplicaciones de Streaming media
- Control de acceso a la web

Ilustración de lo antes mencionado se presenta en la figura 3.1.

Con la diversidad de páginas web y aplicaciones existentes en Internet, es un riesgo real el libre acceso a la navegación sobre todo para usuarios con poco o nulo conocimiento de las amenazas que se encuentran en el exterior.

Las amenazas en la actualidad combinan aplicaciones de registro de tecleo, virus, gusanos, spam, etc. convirtiéndose en vehículos de ataque extremadamente evasivos; sobre todo al usar el correo electrónico o las transferencias de archivos por dispositivos de almacenamiento masivo para difundir juegos, cadenas o aplicaciones de dudosa procedencia que pudieran en su interior contener archivos y aplicativos maliciosos o de dudosa procedencia.

Entre las más comunes e inofensivas formas de infectarse con código malicioso por parte de los usuarios finales están:

- Descargas de archivos.
- Abrir correos infectados.
- Accediendo a los Pop-up.
- Visitando páginas infectadas o hackeadas.
- Instalando aplicaciones Troyanas.

Por otro lado, la ralentización de tráfico o saturación de ancho de banda, es otro factor a tomar en cuenta por parte de los administradores de red. Esta última es muchas veces provocada por usuarios que utilizan los recursos de la empresa para uso de aplicaciones improductivas como Aplicaciones de Mensajería instantánea, P2P, juegos, aplicaciones de Streaming media, etc. Causando la saturación del ancho de banda disponible con actividades que entorpecen el desempeño de las actividades cotidianas de cada empresa.

El uso indebido que se pueda dar a los recursos de la empresa, además de los agujeros de seguridad que se generan con los métodos antes mencionados, hacen ver la importancia del control del tráfico que el administrador de red debe de tener sobre los usuarios, tanto para que los usuarios no caigan en tareas improductivas en las horas laborales, como para que no se ponga en riesgo la seguridad o los mismos recursos que son utilizados para las tareas diarias de cada persona dentro de las empresas.

Los dispositivos UTM tienen la capacidad de controlar el acceso de los usuarios a Internet, esto se puede realizar de muchas maneras, dependiendo de las necesidades existentes y dependiendo de los recursos con los que el usuario final cuente. Existiendo la posibilidad de restringir información selectiva dependiendo de factores determinados por el administrador de red como pudiera ser el tipo de usuario que intenta acceder, el tipo de aplicación o información que se desea consultar, el horario del día en que se intenta establecer la conexión, o simplemente dependiendo de las reglas internas de cada red local.

3.1.1 Técnicas usadas para filtrar contenido web

En un inicio, el control de acceso a las páginas web se realizaba en base a listas de URL's que el fabricante proveía junto con la compra de cada dispositivo, estas listas en un inicio eran bastante simples y poco extensas. Estas eran entregadas a los usuarios para que cada uno fuese agregando direcciones de acuerdo a sus necesidades, por lo que se requería de cada cierto corto tiempo la actualización de las mismas, con el fin de almacenar la mayor cantidad de páginas web para controlar mejor el acceso a Internet de parte de todos los usuarios de la red interna.[18]

La técnica anterior resultaba poco escalable y engorrosa, ya que se requería la actualización manual de cada URL que se deseara bloquear, esto resulta aún más difícil si se tiene conciencia sobre el dinamismo con la que Internet cuenta; ya que se calcula se publican o se renuevan varios miles de nuevas páginas web al día.

Tomando en cuenta los puntos anteriores, los fabricantes iniciaron el almacenamiento de las URL y a proveer actualizaciones periódicas de estas, despreocupando hasta cierto punto a los administradores de red de estar introduciendo manualmente cada URL, y preocupándose únicamente de realizar la actualización cada vez que el fabricante la ponía a su disposición.

Las técnicas usadas por los diversos fabricantes de UTM en la actualidad se presentan a continuación:

- ***Listas de palabras prohibidas:*** este método permite la creación de diccionarios de "listas negras" que contienen palabras o frases. Estas palabras o frases son ingresadas manualmente por los usuarios de acuerdo a sus necesidades, es decir denegando el acceso o permitiendo el mismo hacia URL's en base a su contenido textual. Este método fue el primero en la historia en ser implementado por los fabricantes para dar filtro de páginas web a sus clientes. Sin embargo la efectividad de este método es bastante pobre ya que es fácil de burlar por las mismas amenazas existentes o por los mismos usuarios y es bastante común que se presenten errores en el bloqueo de contenido de las páginas web, por ejemplo un sitio con información médica puede ser bloqueado por considerar que su contenido es ofensivo por contener palabras o frases que han sido incluidas como prohibidas.

- ***Bloqueo de URL:*** esta técnica bloquea o permite el contenido de URL´s definidas, muchas veces el fabricante provee listados con URL's comunes que son consideradas como ofensivas o confiables, dependiendo de la técnica que se esté

[18] http://www.wikipedia.org, sitio consultado en julio de 2008

utilizando ya sea la de denegar todo y permitir lo conocido o permitir todo y denegar lo ofensivo. Estas suelen contar con actualizaciones por parte de los fabricantes para garantizar el control a los administradores de red. Sin embargo muchos fabricantes dejan abierta la posibilidad que los mismos usuarios definan las páginas que quieren permitir o denegar según sea el caso, ya que estos no proporcionan listas de URL para sus clientes. En ambos casos se requiere yo continua actualización de las listas para siempre tener un control de acceso seguro a Internet.

- ***Bloqueo por categoría:*** es la nueva tecnología usada para el filtrado de páginas web, con ella se han obtenido grandes resultados en el proceso de filtrado sin realizar grandes procedimientos en la configuración de los dispositivos. Esta técnica utiliza servicios externos que almacenan los listados de URL ya no clasificadas por palabras o frases sino por su contenido estructural, para esto se requiere que cada vez que se genere una nueva petición de acceso a alguna dirección web, esta tenga que ser consultada con los servidores externos manteniendo así actualizada la base de datos que sirve para controlar el acceso a Internet. Generalmente los dispositivos UTM utilizan cache para almacenar las páginas web que ya han sido accesadas, para que la próxima vez que se realice la petición a esta misma no se tenga que nuevamente consultar con los servidores externos, sino que ya se tiene registro de la categorización de la misma, permitiendo un acceso de manera más rápida, logrando así una mejor utilización de ancho de banda.

  Otra característica de este método es la relativa facilidad de configuración con la que cuenta, en la que el usuario únicamente se preocupa de indicar los márgenes que quiere verificar, un ejemplo de esto mostrado en la figura 3.2, mientras que el equipo junto con las bases de datos externas se encargan de mantener actualizadas y en orden las bases de datos que muchas veces están distribuidas por cada fabricante en distintas partes del mundo. La única limitante es que por tratarse de una característica dinámica, se requiere tener al día las licencias proveídas por los fabricantes las que implican un costo monetario adicional cada cierto tiempo.

De las tres técnicas de filtrado web antes mencionadas, la que ofrece mayor facilidad y mejores resultados es la de bloqueo por categoría, sin embargo las dos primeras también son utilizadas como complemento de la última ya que muchas veces se requiere el acceso/denegación de una página web en especifico, por ejemplo si en una institución se necesita tener bloqueados los accesos a las páginas web de organizaciones financieras alrededor del mundo pero se necesita el acceso única y exclusivamente a una de ellas, es

más fácil denegar el acceso a todas las organizaciones financieras usando el bloqueo por categoría pero agregando en la lista de URL permitidas a la dirección que se requiere poder acceder en especifico.

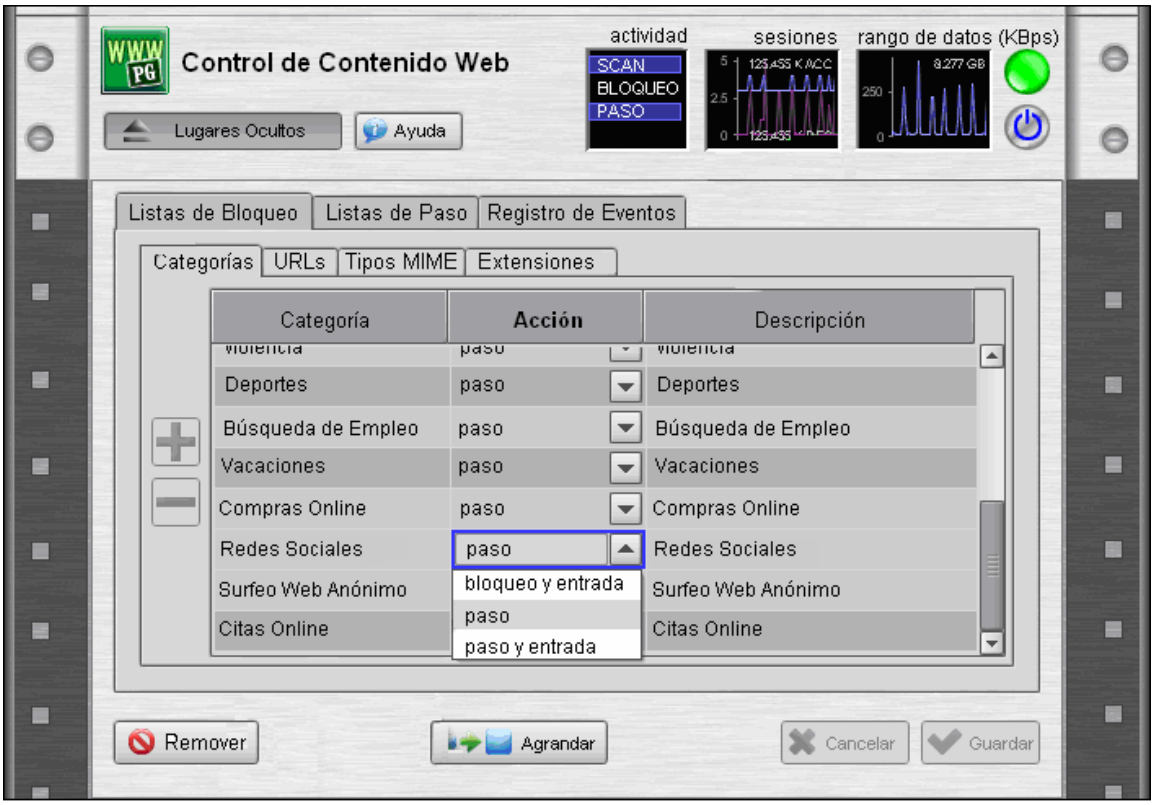


Figura 3.2 Ilustración de una configuración de filtro de contenido web.

3.2 Regular acceso de los usuarios a Internet

Una vez solventado el tema del control de acceso de páginas web en Internet, se ve la necesidad de aplicar estas políticas de control a los usuarios de la red interna. Ya se sabe que en cada institución existen diversos usuarios, con diferentes tareas asignadas, diferentes niveles de conocimientos informáticos y diferentes necesidades. En la figura 3.3 se ilustra una estructura típica de red, con diversos departamentos conectados entre sí al dispositivo UTM.

Se pudiese tener un solo perfil de protección para toda la red, a pesar que es la configuración quizá más sencilla pero no es lo más recomendable, ya que no se le puede dar el mismo nivel de acceso a una persona con pocos conocimientos de informática, como se le da a una persona que trabaja en el departamento de tecnología, o a alguien que trabaja en el departamento financiero.

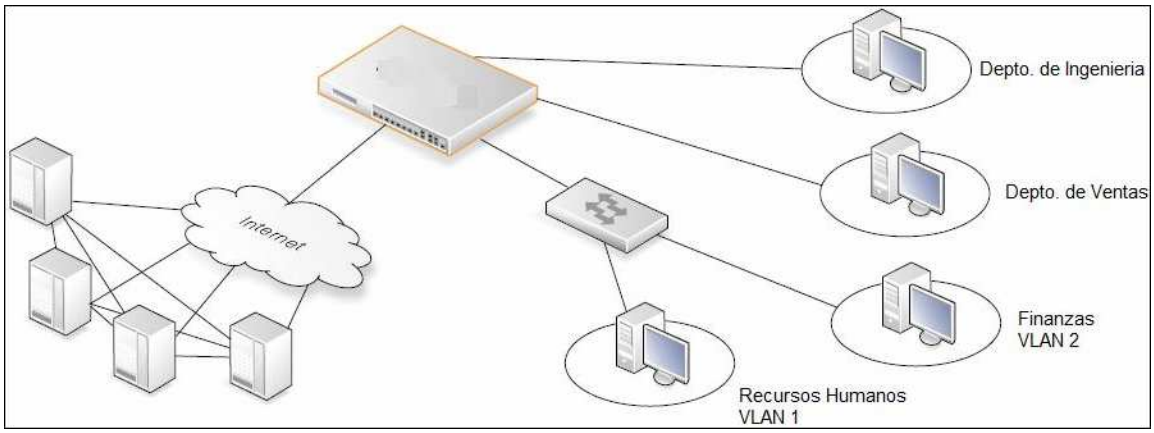


Figura 3.3 Ilustración de una red con diversidad de perfiles de usuarios.

En un inicio la configuración del control de acceso a Internet se daba bajo un solo perfil de protección, sin embargo esta técnica ha ido evolucionando tratando de ser más granular o personalizado el control de navegación, al mismo tiempo se ha buscado la integración de herramientas que permitan manipular a usuarios independientes o a grupos de usuarios de manera general.

Por lo general los usuarios se agrupan en perfiles de acuerdo a su rol o función en la empresa, es común agrupar usuarios por departamento o por nivel de jerarquía, una vez estos agrupados se aplican las políticas respectivas para cada uno de ellos. De igual forma es posible la agrupación de usuarios si el dispositivo soporta autenticación de los mismos.

En la tabla 3.1 se muestra un posible ejemplo de agrupamiento de IP y de usuarios.

IP Gerencias
192.168.1.2
192.168.1.3
192.168.1.4
192.168.1.5

IP Area Tecnica
192.168.2.41
192.168.2.42
192.168.2.43
192.168.2.44
192.168.2.45

IP de ventas
192.168.2.11
192.168.2.12
192.168.2.13
192.168.2.14
192.168.2.15

IP Finanzas
192.168.21
192.168.22
192.168.23
192.168.24
192.168.25

Usuarios	Password
lcalderon	********
jmejia	**********
cgonzalez	******
maviles	********
wmoran	******
chernandez	*******
dlinares	******
vcruz	*****
nlopez	*******
falvarez	*****
hnovoa	******
kretana	********

Tabla 3.1 Muestra de agrupación de usuarios por IP y por nombre de usuarios

Estas políticas pueden determinar el control del acceso a Internet o a determinadas aplicaciones, basándose en la IP origen, en la IP o URL destino, en el usuario o grupo de

usuarios que realice la petición o incluso en el horario/fecha en el que ha sido hecha la consulta.

3.2.1 Modalidades de configuración de usuarios

La configuración más común es la que controla en base a la IP de los usuarios, para ello se requiere colocar IP fijas por usuarios o por áreas de trabajo, restringiendo que el usuario pueda alterar o modificar la IP que ya tiene asignada. Una vez cubierta esta parte se procede a agrupar las IP y a establecer políticas comunes para cada grupo en base a las necesidades de cada grupo. Un posible punto de fallo es que las IP generalmente se asignan a maquinas definidas por lo que si un usuario consigue ingresar a otra PC diferente a la suya podría cambiar totalmente su perfil y acceder libremente a la web.

Otra configuración bastante usada es la de controlar el acceso a IP's o URL's determinadas, esto se puede aplicar tanto a usuarios individuales como a grupos en base a su IP o a su nombre de usuario, para esto se quiere tener bien definidas las URL a las que se requiere restringir el acceso y cubrir las posibles variantes de estas mismas.

Una técnica no tan conocida pero que muchos fabricantes optan por tomar en cuenta por su versatilidad y seguridad es la de controlar acceso web en base a la autenticación de usuarios o los nombres de registro de usuarios, es decir una persona puede utilizar cualquier maquina de la red pero para empezar necesita escribir su nombre de usuario y su contraseña, con esto se asocian dichos parámetros a los perfiles hechos, haciendo aún más difícil el suplantar identidades. Para esto se requiere un buen sistema de registro y control de usuarios que bien pudiera ser proporcionado por los UTM o por bases de datos externas que se pudieran conectar a estos dispositivos tales como el Active Directory de Windows, servidores Radius, etc.

Para el caso de se necesite enmarcar actividades en horas o fechas definidas, estas se pueden aplicar de la misma manera a usuarios o grupos de usuarios en base a IP o a nombre de usuarios. Muchas veces estas aplicaciones se suelen utilizar para dar libre acceso o un acceso no tan restrictivo en horas definidas del día como la hora del almuerzo o la hora de la salida. De la misma manera si se tuviera una video conferencia en fechas establecidas se pudiera controlar el acceso a aplicaciones que demanden grandes anchos de banda por parte del resto de los usuarios, y permitiendo que dicha aplicación acapare el mayor porcentaje de disponibilidad de la red. En la figura 3.4 se muestra una ilustración de la versatilidad con la que cuenta la aplicación de políticas en un dispositivo UTM.

Figura 3.4 Ilustración de la versatilidad con las que puede contar un dispositivo UTM.

3.3 Sistemas de seguridad en la red

Dependiendo del fabricante se puede incluir el término de IDS e IPS en un mismo dispositivo, en la actualidad se acostumbra a complementar ambos términos, se utilizan los IDS como principales actores de este proceso identificando las posibles anomalías que viajen por la red, dejando la restricción de aplicaciones maliciosas a IPS siempre y cuando hayan sido identificadas o categorizadas previamente.

De la misma manera se provee seguridad con los sistemas Antivirus y Antispam, los métodos de identificación de anomalías entre estos son muy similares motivo por el cual se estudiaran en conjunto en este apartado. Estos sistemas Antivirus comúnmente son llamados NAV (Network Antivirus) debido a que su seguridad es perimetral por encontrarse en un dispositivo de similares características.

Los sistemas pueden implementar sistemas de protección donde se permite todo y se deniegan las amenazas conocidas o donde se deniega todo y se permite únicamente las aplicaciones conocidas, esto dependerá de las necesidades o los gustos del cliente final. Sin embargo el más recomendable, es el de negar todo y únicamente permitir las aplicaciones a utilizar.

3.3.1 Identificación de tráfico (IDS)

Estos sistemas de IDS/IPS y Anivirus/Antispam incorporan modernos sistemas de control con amplia gama de técnicas para la detección de código malicioso. Dentro de esta etapa de identificación de tráfico se suelen utilizar diversas técnicas entre las que se pueden mencionar:

- Verificación de integridad: se emplean funciones unidireccionales Hash y firmas digitales para verificar la integridad de los datos. Sobre todo con sistemas que utilizan funciones criptográficas Hash débiles como MD5 o vulnerabilidades que busque alterar bases de datos de los sistemas internos, por mencionar algunos ejemplos.

- Reconocimiento de firmas o patrones de ataque: se comparan las actividades en curso con patrones conocidos denominados firmas de ataque como pudieran ser:

    - Similitudes entre direcciones IP origen y destino en un mismo paquete.
    - Escaneo de puertos, paquetes de un mismo origen a distintos host destino
    - Evaluación de cadenas claves como login o password.
    - Inspección de archivos adjuntos o aplicaciones que se intenten intercambiar por correo electrónico. (HAV)

  Sin embargo utilizando este método, se tiene el inconveniente de no poder detectar anomalías que no coincidan con los registros de firmas, por lo que es necesario el pre-proceso de reemsamblar los paquetes IP fragmentados; así mismo de analizar las cabeceras de los paquetes en busca de exploraciones de puertos o inundaciones SYN, analizando el campo de datos en busca de código malicioso.

- Detección de anomalías: se crean perfiles de la actividad de usuario normal. Siendo posible así detectar desviaciones de ese perfil. Utilizando para esto redes neuronales, inteligencia artificial, mapas de auto-organización y métodos estadísticos o heurísticos. Con la única salvedad que el encargado de configurar estos perfiles debe conocer a cabalidad el tipo de tráfico que se utiliza en la red para evitar generar una alta tasa de positivos.

La mejor forma de brindar medidas de seguridad en la red es utilizando las tres técnicas antes mencionadas. Esto con el objetivo de generar la menor cantidad posible de falsos positivos pero sobre todo de falsos negativos, ya que son estos últimos las amenazas que se pasan por alto y se les da vía libre a la red interna.

El sistema IDS tiene su principal función en identificar el tipo de tráfico como conocido o desconocido y en base a esto informar de las anomalías percibidas. Es importante aclarar que hasta este punto no se está bloqueando o permitiendo nada únicamente se está identificando el tipo de tráfico que está percibiendo el dispositivo UTM.

3.3.2 IPS y Antivirus

El trabajo complementario que procede luego de identificar al tráfico es el de permitir o denegar este hacia la red interna, esta es la función de IPS. Generalmente esta opción viene desactivada por defecto, es decir se identifica el tráfico y se tiene la opción en base a lo identificado de dejar pasar o denegar las anomalías o el tráfico malicioso que se detecte en la red. Las principales acciones tomadas por estos dispositivos se describen a continuación:

- Los IPS reaccionan de forma automática a las alarmas ya sea reconfigurando las políticas del firewall, actualizando las listas negras del dispositivo, bloqueando puertos o simplemente bloqueando lo desconocido.

- Utilización de Honeypots - Honeynets: los cuales son trampas para atraer atacantes y analizar sus ataques; estos asignan espacio de direcciones no utilizados en un host sin información sensible pero de atractiva apariencia a los atacantes. Muchas veces simulan servidores Proxy. El objetivo de estos es que los atacantes no puedan distinguir entre un Honeypot y un host normal, comúnmente son utilizados para distraer la atención de los atacantes de las maquinas más importantes del sistema para tratar de recoger la mayor cantidad de información como evidencia a fin de identificar nuevos ataques. La mezcla de varios Honeypots conforman una Honeynet que no es más que un conjunto de host con falsa relevancia. En la figura 3.5 se observa una ilustración de estos dispositivos.

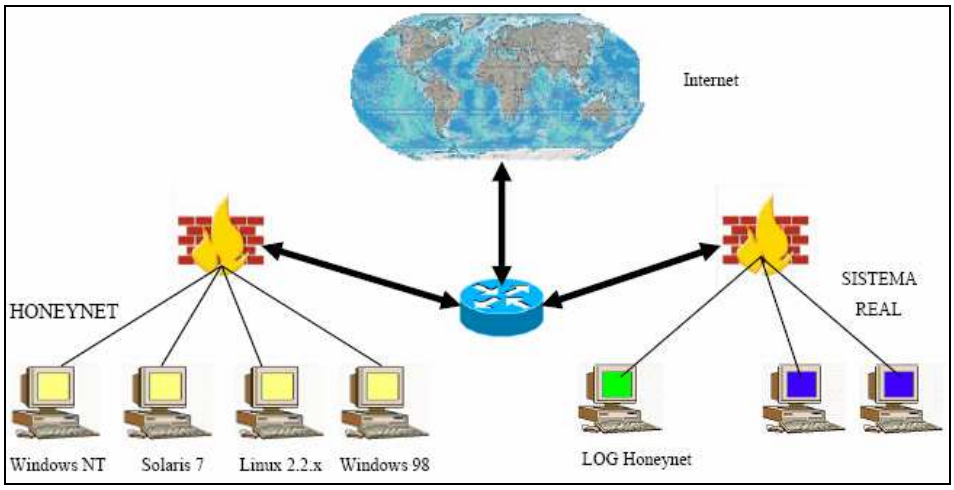


Figura 3.5 Ilustración de Honeypots y Honeynet[19]

- Implementación de Tarpits: similares a los Honeypots ya que atraen a sus atacantes simulando ser host con recursos vulnerables. Sin embargo el objetivo de estos es retardar al atacante la mayor cantidad de tiempo posible bloqueando los recursos del mismo, esto con el fin de caducar los tiempos de espera de los atacantes generando así una red más segura. En la figura 3.6 se muestra una maraña de links creada por un Tarpit.

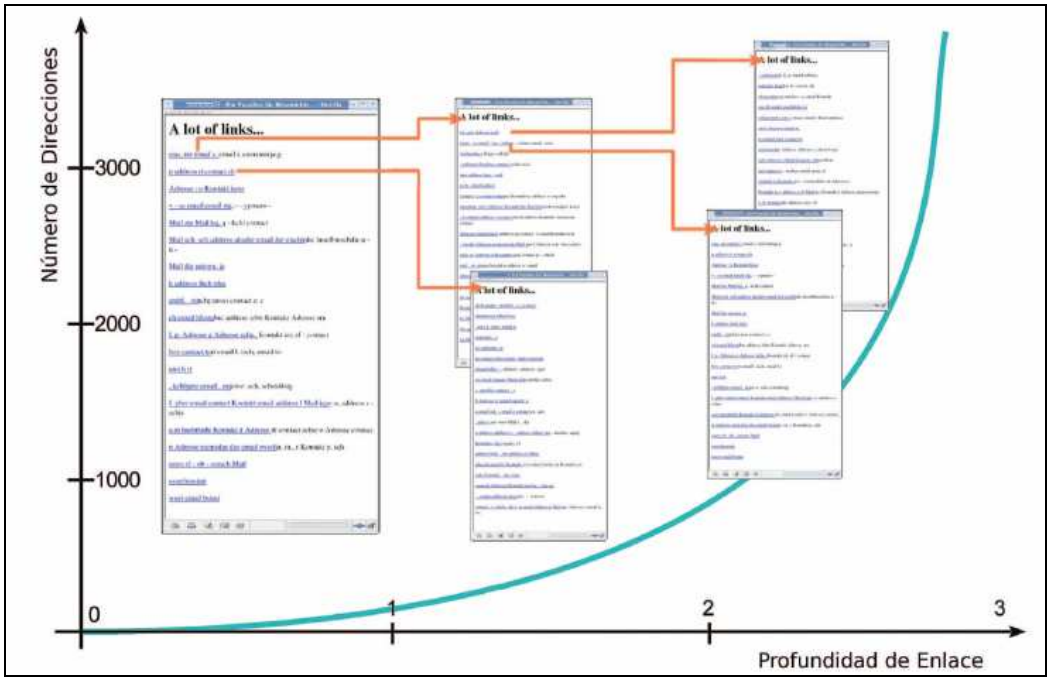


Figura 3.6 Ilustración de links creada por un Tarpit.[20]

[19] http://www.dea-es.com, enlace consultado en junio de 2008

Es importante aclarar que el tipo de tráfico que viaja cifrado es difícilmente identificado en su totalidad, únicamente se marca como tal y por defecto suele dejarse pasar hacia la red interna. Pero lo más recomendable es conocer los posibles remitentes de tipo de tráfico hacia la red interna, una vez teniendo claro este punto se puede permitir o denegar con más propiedad el tráfico identificado.

De la misma manera una parte de seguridad es proporcionada por los sistemas Antivrus-Antispam de estos dispositivos. A diferencia de los sistemas IDS/IPS, los sistemas antivirus se enfocan directamente en las aplicaciones o archivos que ingresan a la red interna, sin embargo los métodos de detección de anomalías como se menciono con anterioridad son bastante similares a los de IDS/IPS. En la figura 3.7 se presenta una ilustración de sistemas Antivirus en un UTM.

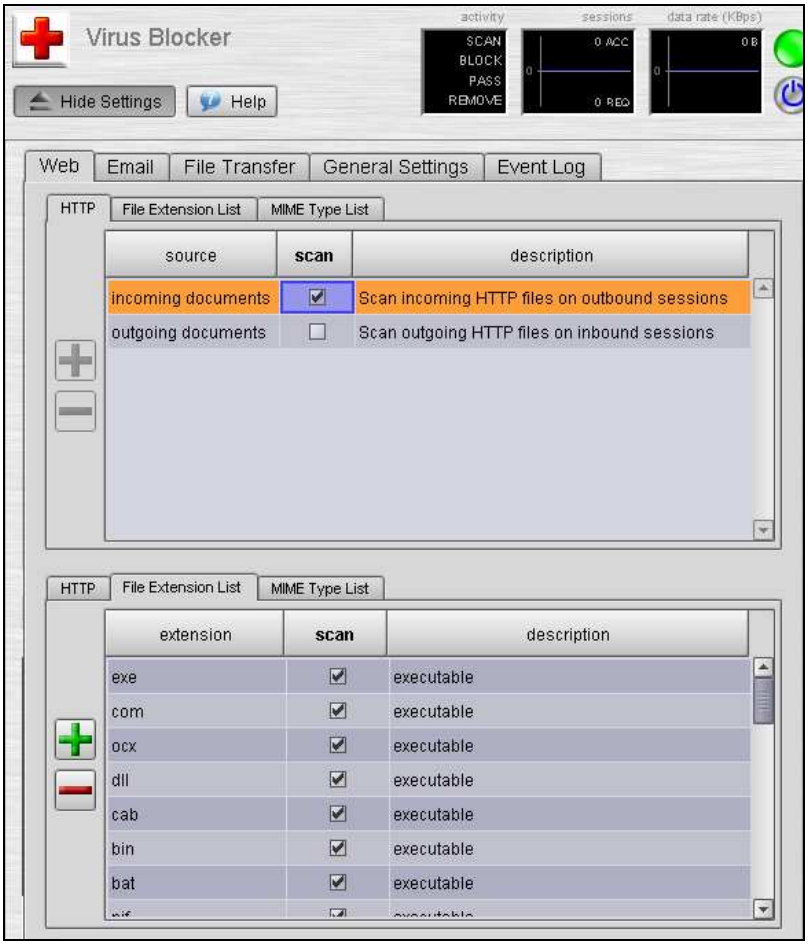


Figura 3.7 Ilustración de sistemas antivirus.

[20] http://www.linux-magazine.es, enlace consultado en junio de 2008

Ambos sistemas, utilizan bases de datos para almacenar registros de ataques o antivirus según sea el caso, es importante mencionar la ventana de vulnerabilidad a la que ambos sistemas se ven sometidos una vez se identifica una nueva amenaza o virus en cada dispositivo, ya que esta es almacenada en las bases de datos propietaria, y se requiere de un tiempo variable para estas sean registradas y actualizadas a todos los equipos de dicho fabricante (Amenaza del día cero).

3.4 Creación de VPN confiables.

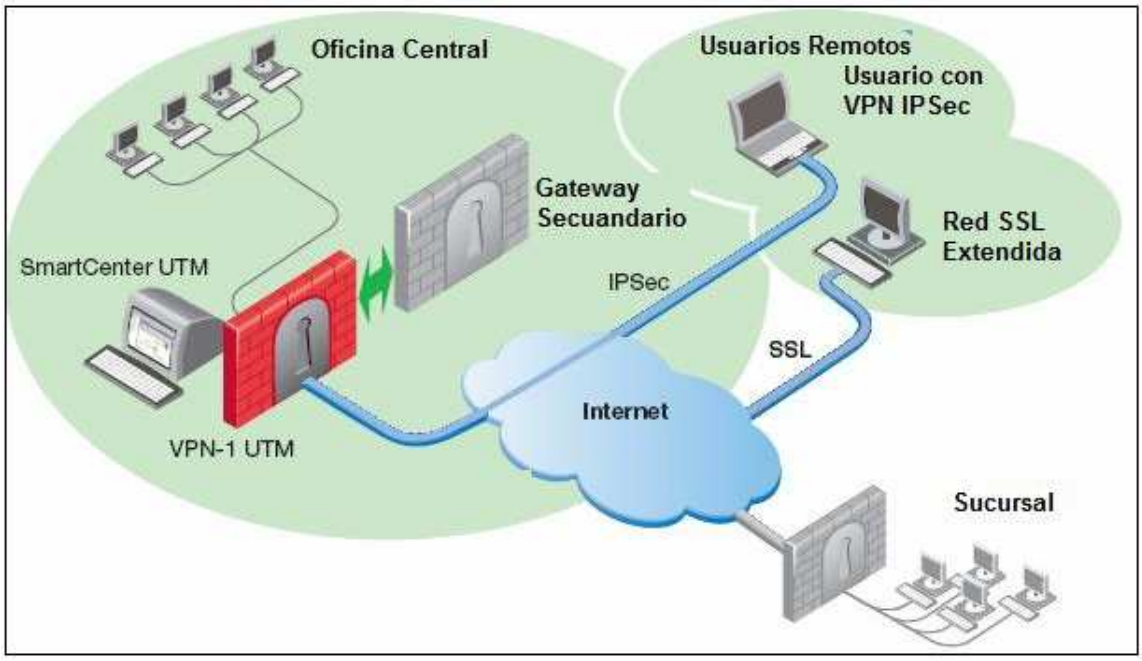


Figura 3.8 Ilustración de esquema de VPN creadas por UTM

Una VPN es un circuito lógico seguro que se crea entre dos o más redes separadas físicamente entre sí. Estas utilizan mecanismos de encriptación y autenticación para asegurar que solo los usuarios autorizados tengan acceso a la información que por ellos se transmite.

Como se observa en la figura 3.8 la creación de VPN en los UTM son de mucha utilidad si se requiere el acceso remoto a la LAN de manera segura generando confidencialidad de datos, integridad y autenticación entre los puntos involucrados. Estos dispositivos en su gran mayoría, en la actualidad cuentan con dos posibles configuraciones de accesos remotos, VPN SSL y VPN IPSec.

3.4.1 VPN SSL

La creación de VPN SSL (Secure Socket Layer) ofrece la ventaja de generar un canal lógico de comunicaciones seguro entre un cliente y un servidor con la posibilidad de ser independiente del sistema operativo usado por ambos, además que se pueda utilizar sin ningún software especial más que un browser o navegador del lado del cliente, junto con un sistema de autenticación que facilite el uso o el acceso al servidor o red remota.

En la actualidad SSL ha logrado tener múltiples aplicaciones en el mundo de las redes informáticas, a tal grado de ser frecuentemente utilizado en transacciones bancarias, aplicaciones web, transferencias de archivos, etc. En la tabla 3.2 se presenta un cuadro ilustrativo de los diversos aplicativos SSL con su número de puerto respectivo, que la IANA (Internet Assigned Numbers Authority) ha definido como estándar para su uso.

Identificador	Puerto TCP	Descripcion
HTTPS	443	HTTP sobre SSL
SMTPS	465	SMTP sobre SSL
NTTPS	564	NTTP sobre SSL
TELNETS	992	TELNET sobre SSL
IMAPS	993	IMAP sobre SSL
IRCS	994	IRC sobre SSL
POP3S	995	POP3 sobre SSL
FTPS-DATA	989	FTP Datos sobre SSL

Tabla 3.2 Ilustración de aplicaciones con SSL[21]

Los dispositivos UTM una vez configurados permiten la facilidad de seleccionar el tipo de aplicativos que se quieren acceder desde la web (FTP, HTTP, telnet, etc.), de la misma manera este dispositivo es capaz de segmentar a cada usuario según sus privilegios. En la figura 3.9 se presenta el acceso que este tipo de VPN utiliza para el usuario final, en donde solo se requiere un navegador y una autenticación para lograr acceder a la red interna de manera segura.

Este tipo de conexión es ideal para usuarios ocasionales o usuarios móviles, es muy usada por empleados con movilidad que requieren acceder de manera segura a los recursos centrales de la red sin importar el sitio desde donde se requiera el acceso, este puede ser la computadora personal del empleado o ejecutivo de la empresa o desde un host ubicado en un cibercafé, ya que el tipo de protocolo de seguridad que se establece se da a nivel de aplicación y no se requiere ninguna otra configuración especial en el host remoto.

[21] SSL y Otros Protocolos Seguros, documento consultado en mayo de 2008

En el dispositivo UTM únicamente se requiere configurar parámetros de autenticación por cada usuario, el tipo de aplicaciones a las que se tendrá acceso y el segmento de red o host a los cuales se podrán conectar desde fuera.

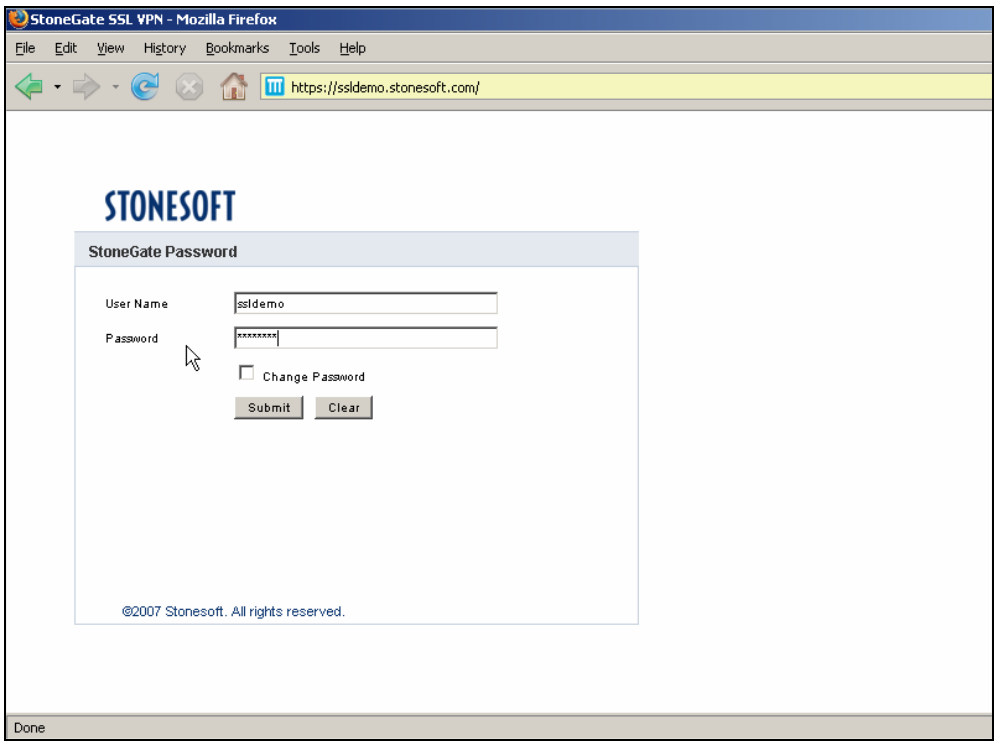


Figura 3.9 Ilustración de autenticación para una VPN SSL.

3.4.2 VPN IPSec

IPSec tiene como función proveer seguridad de autenticación y cifrado en nivel de IP. Garantizando así la conexión segura entre múltiples sistemas de banda ancha, pudiendo utilizar diferentes algoritmos criptográficos para transferir de forma segura la información e incluso utilizar varias trayectorias para establecer la comunicación entre un par de host.

Esta técnica requiere tanto de una aplicación de servidor como de una aplicación de cliente instalada en los puntos a interconectar. Esto debido a que la negociación entre ambos puntos es la que define el tipo de cifrado y las vías a utilizar para crear el túnel de comunicación.

Para el caso de los UTM, se recomienda colocar en cada sitio a interconectar uno de estos dispositivos para enlazar los puntos entre sí de manera segura, sin embargo si se requiriese únicamente la conectividad entre un host y un segmento de red, se puede utilizar un cliente

de IPSec en el host e instalar un UTM en el sitio central, de igual manera si únicamente se requiriese la interconexión de dos host, se podrían utilizar versiones software de cliente y servidor de IPSec. Lo anterior se ilustra en la figura 3.10.

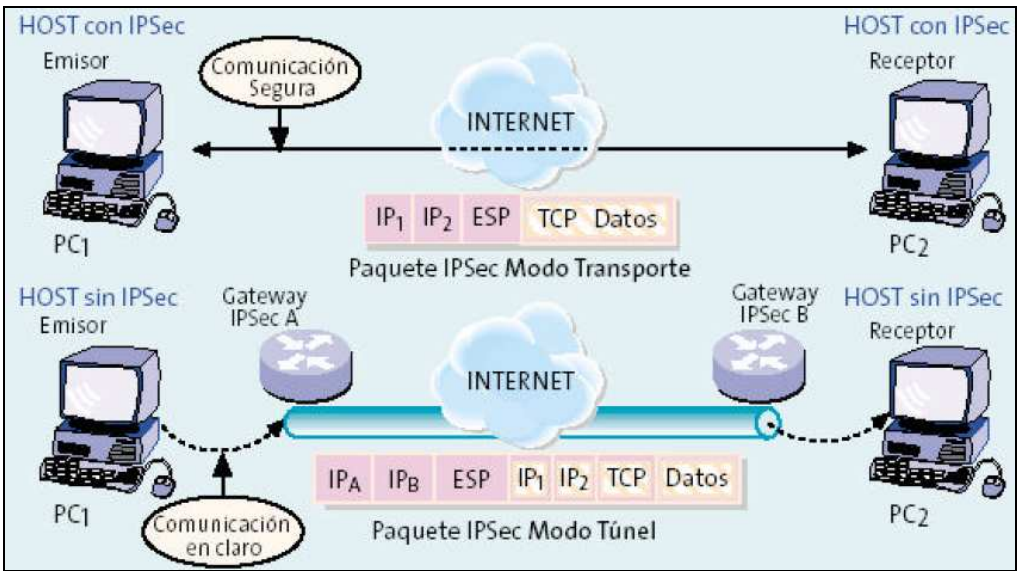
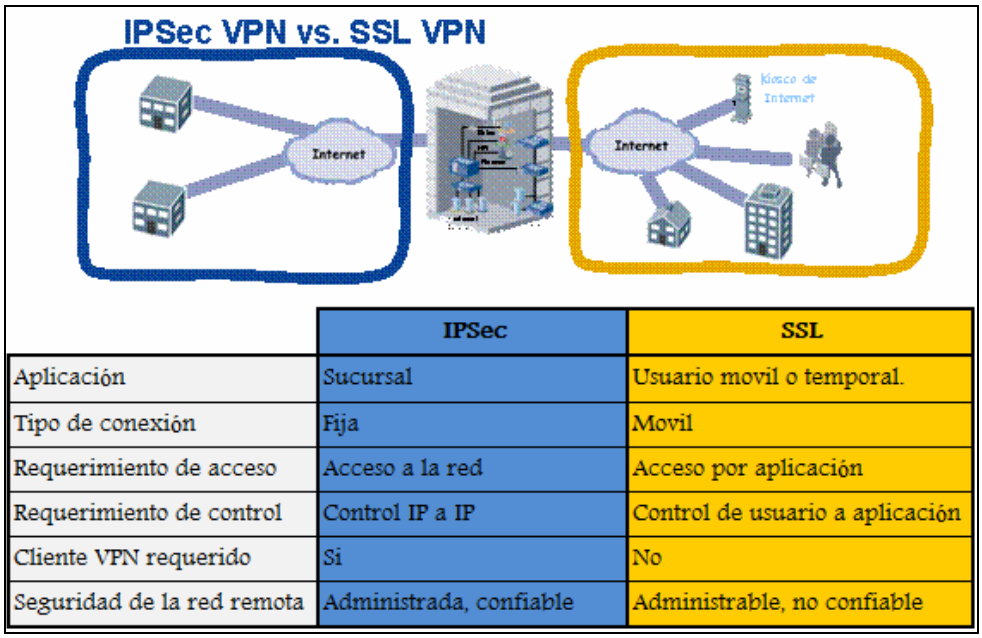


Figura 3.10 Ilustración de VPN IPSec

Para este caso el tipo de configuración que se necesita en los dispositivos UTM involucrados implica diversos factores como la IP que se comunicará en el tunel, el método de autenticación a utilizar entre los equipos, la clave de cifrado definida por el usuario (debe ser la misma en ambos puntos), el rango de IP de las LAN que se verán involucradas en la conexión, finalmente se configuraran el tipo de servicios requeridos y los perfiles requeridos por cada uno de los equipos. En la figura 3.11 se muestra una comparación directa entre ambos tipos de VPN.



	IPSec	SSL
Aplicación	Sucursal	Usuario movil o temporal.
Tipo de conexión	Fija	Movil
Requerimiento de acceso	Acceso a la red	Acceso por aplicación
Requerimiento de control	Control IP a IP	Control de usuario a aplicación
Cliente VPN requerido	Si	No
Seguridad de la red remota	Administrada, confiable	Administrable, no confiable

Figura 3.11 Comparacion entre VPN IPSec y SSL.

3.5 Complementos Adicionales

En los apartados anteriores de este capítulo se enfocaron las principales aéreas que los dispositivos UTM administran, sin embargo estas no son las únicas, sino que dependiendo del fabricante y/o modelo de equipo pudieran ser muchas más las versatilidades o aplicaciones que estos pudieran cubrir.

3.5.1 Aplicaciones P2P/IM

El control de ambos tipos de aplicaciones es muchas veces la principal preocupación de los administradores de red, en el caso de P2P por la saturación del ancho de banda y en el caso de IM por la cantidad de archivos peligrosos que pudieran transferirse de esta manera o por la cantidad de tiempo que los empleados pudieran estar desperdiciando durante la jornada de trabajo.

La mayoría de UTM ofrece el control de aplicaciones P2P/IM bajo el mismo estándar de las demás aplicaciones, es decir aplicando políticas restrictivas o permisivas para usuarios o grupos de usuarios en base a su IP o a su nombre de dominio.

Sin embargo por el comportamiento y el desempeño que estas aplicaciones han tomado en nuestros días, entre las cuales se puede mencionar que una aplicación P2P si es bien utilizada puede ser beneficiosa para el mismo desempeño laboral de algunos empleados, sobre todo de los que son más conocedores del área informática. Por el otro lado una aplicación IM pudiera funcionar como un medio de comunicación más entre los mismos empleados o contactos laborales.

En base a lo anterior también existen opciones alternas a la simple permisión o denegación de servicios, es decir las de un control más granular que permiten en el caso de P2P:

- Controlar el máximo y mínimo ancho de banda que se pudiera utilizar para diversos tipos de aplicaciones P2P.

- Administrar una variedad de aplicaciones P2P de manera individual (Kazza, BitTorrent, Ares, Gnutella, Skype, etc.).

- Regular el tipo de archivos que se pueden acceder desde estos aplicativos.

Similar panorama se presenta para la aplicación IM, entre las políticas especiales tenemos:

- Regulación de usuarios en base a cuentas personales de aplicaciones IM (Yahoo, MSN, AOL, etc.).

- Control de extensiones de archivos que se pudieran transmitir en una ventana o carpeta de IM.

Para complementar estas políticas especiales también se pueden aplicar las políticas con las que se utilizan con las aplicaciones más comunes, como manejo por IP, por nombre de usuario o grupo de usuarios, manejo de aplicaciones por hora/fecha. De igual manera se almacena el registro de estas aplicaciones, sin embargo muchas veces se requiere de dispositivos externos para almacenamiento de información, sobretodo de aplicaciones IM ya que algunos dispositivos son capaces de almacenar todas las conversaciones que se generaron en un tiempo determinado. En la figura 3.12 se presenta una ilustración del manejo de aplicaciones P2P en un UTM.

Figura 3.12 Ilustración de administración de aplicaciones P2P.

3.5.2 Reportes.

Los dispositivos UTM capturan el total de tráfico entrante y saliente de la red, con estos registros es posible generar reportes dependiendo de la necesidad del cliente ya que se cuenta con el recurso primario que es el logeo de todas las actividades que lleguen hasta el dispositivo y la totalidad del tiempo que esté conectado a la red.

Estos pueden ser usados por los administradores de estos equipos para monitorear el desempeño de la red a lo largo de un período determinado de tiempo, de la misma manera pueden ser usados para determinar la causa de una posible falla o la fuente/destino de alguna aplicación o tráfico anómalo que se estuviera generando en/hacia la red interna.

En algunos casos estos UTM cuentan con capacidades para generar por si solos estos reportes con ciertas limitantes de información o de tiempo de operación, en algunos otros casos necesitan de otro dispositivo especializado para la generación de reportes con una

calidad superior a los primeros y en un tercer caso cuentan con la capacidad de interconectarse con equipos generadores de reportes como syslog para que en conjunto se puedan generar estos tan útiles registros de red.

Debido a la universalidad que en los últimos años ha caracterizado a los archivos en formato PDF, gran parte de fabricantes ofrecen como primera opción este formato para presentar en su totalidad los reportes. En la figura 3.13 se presenta una ilustración de la generación de un reporte desde un UTM.

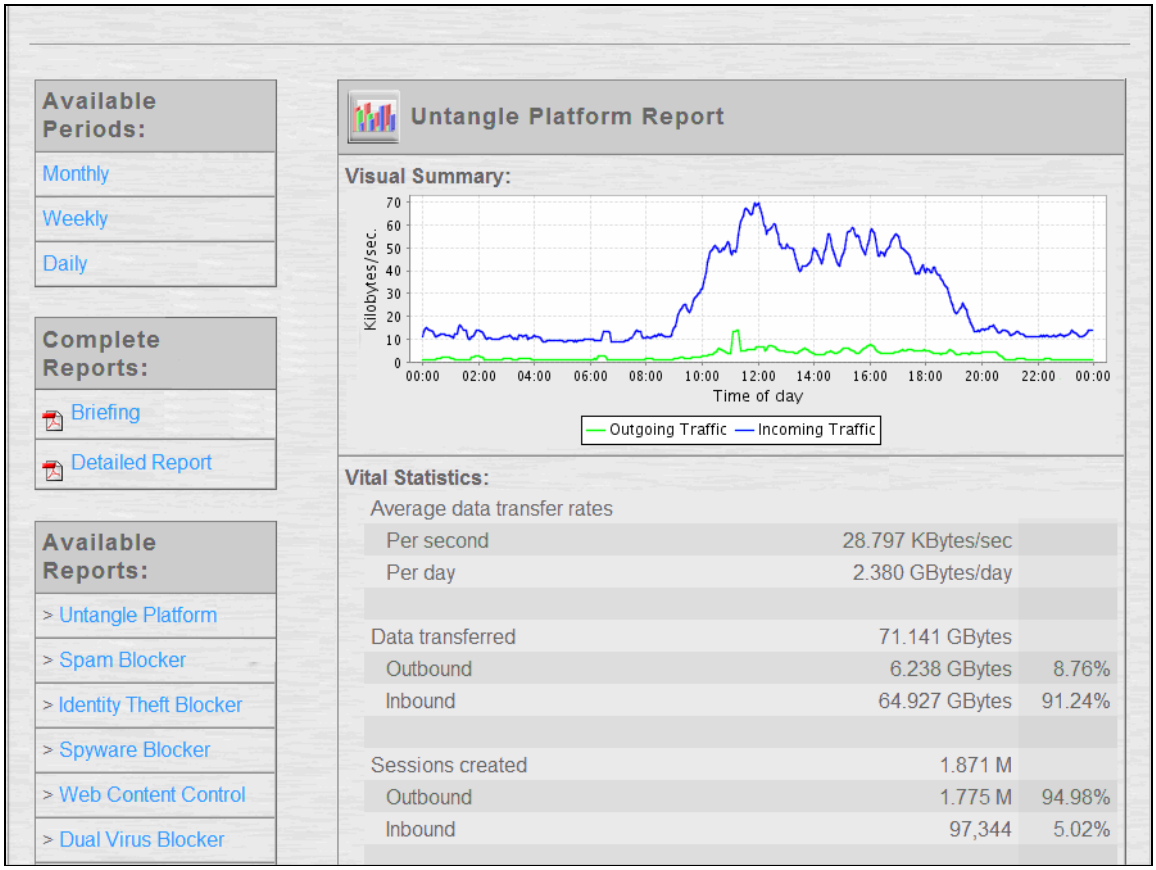


Figura 3.13 Ilustración de un reporte generado.

Capitulo 4: Introducción

En el siguiente capítulo se realiza en un inicio, el detalle de las pruebas a realizar así como una descripción de los equipos a utilizar, los cuales para el caso serán dos equipos de diferentes fabricantes, se utilizara un equipo Fortinet en primer lugar y un equipo SonicWALL posteriormente.

Luego de esto se mencionaran los apartados de cada uno de ellos y sus principales funciones. Describiendo con un poco más de detalle los apartados de más importancia a nuestro estudio como lo son:

- Descripción general.
- Control de usuarios.
- Creación de VPN.
- Control de Acceso Web.
- Control de Amenazas.
- Creación de Reportes.

Se realiza la descripción de estos apartados de manera separada en los equipos, para posteriormente realizar una especie de comparación entre ambos y presentar una tabla para cada sección mostrando los apartados que pueden ser configurados en cada uno y explicando de ser necesario, el equipo que desempeño un mejor resultado en las mismas.

4.0 COMPARACIÓN ENTRE DISPOSITIVOS UTM.

Los sistemas de gestión unificadas de amenazas, se han convertido en un importante elemento para garantizar la protección perimetral de cualquier empresa o corporación. En gran parte debido a que en lugar de aplicar varios elementos diferentes para lograr las diversas capas de protección en la conexión hacia el exterior, resulta más eficaz, compacto, y con ello barato, colocar un elemento que agrupe la mayoría, o todas las funciones necesarias para poder controlar potenciales amenazas y los aplicativos a los que se accederá de la red interna.

4.0.1 Introducción.

El empleo de un dispositivo de seguridad ofrece la indudable ventaja de usar un hardware idóneo, normalmente reducido al mínimo, y colocar el software específico destinado a cubrir diversos aspectos de seguridad. En lugar de emplear una PC, o un servidor, convencionales para montar sobre el mismo un sistema operativo estándar y luego diversas aplicaciones de seguridad, el UTM parte de un circuitería reducida, en la que se excluye todo elementos que puedan causar fallos o dejar abiertos puertos no deseados.

La composición de los diversos elementos de seguridad que se colocan sobre un determinado equipo es notablemente amplia y varía mucho para cada fabricante e incluso dependiendo de series o modelos. El elemento más básico es un cortafuegos o firewall, que es el elemento primordial para establecer una defensa perimetral de red. Luego, capa sobre capa, se colocan otras funciones, como antivirus, anti spam, detección de vulnerabilidades y filtrado selectivo de contenidos Web. Los más sofisticados realizan un importante control a nivel de contenidos que permite proteger la salida de la empresa de determinados tipos de documentos, de cara a proteger la propiedad intelectual interna.

Los primeros firewall que incluían características de UTM se dan a finales de los años noventas, desde esa fecha hasta la actualidad ha proliferado de manera considerable el número de fabricantes de estos dispositivos en el mercado, a continuación se presenta un listado de algunos de ellos: BorderWare, Check Point, DLink, Fortinet, Impreva, Interfex, Juniper, Ntsecurity, SonicWALL, Symantec, Watchguard, Zyxel, etc.

Con el fin de ilustrar de una mejor manera los equipos sometidos posteriormente a las pruebas evaluativas, se presenta una breve descripción de las características de estos, describiendo de manera general su estructura y sus aplicativos.

4.1 Pruebas de equipos.

4.1.1 Pruebas a realizar.

En un inicio se procederá a realizar la familiarización con los equipos, visualizando de manera general las opciones que estos dispositivos ofrecen a los usuarios. Para lo cual se utilizara un cuadro de cotejo con el objetivo de estandarizar las principales utilidades que estos dispositivos ofrecen, en la tabla 4.2 se presentan los criterios a utilizar.

Para las pruebas se utilizaran por un lapso de alrededor de 10 días un promedio de 20 usuarios en sus actividades normales, con el objetivo de evaluar el equipo en un ambiente laboral real, las pruebas y configuraciones del equipo se realizaran en horas de poco tráfico o poca actividad laboral. Utilizando el escenario mostrado en diagrama 4.1, en donde se observan enlaces redundantes entre dos IPS con un solo segmento LAN y con la necesidad de utilizar VPN temporales.

En el diagrama 4.1, se muestra el esquema de configuración a utilizar en las pruebas.

Cuadro Comparativo de Dispositivos UTM											
	Firewall	Perfiles	IDS	IPS	Antivirus	Antispam	VPN	IM & P2P	Filtrado	Logs	Reportes
SONICWALL											
FORTINET											

	Areas	NAT	HA	Throughput	RAM	VDOM	Consola	Interfaces	R. Dinamico
SONICWALL									
FORTINET									

Tabla 4.1 Criterios generales a evaluar.

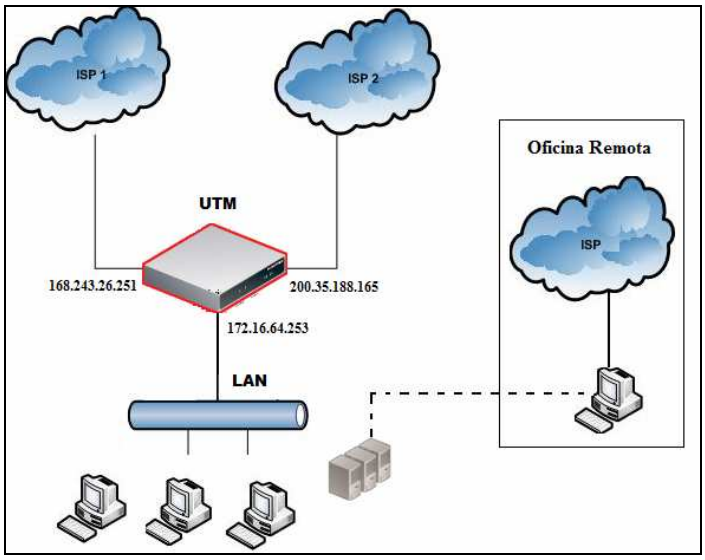


Diagrama 4.1. Esquema a utilizar en las pruebas.

Una vez identificados los criterios generales antes mencionados, se presentaran evaluaciones para cada apartado haciendo un estudio más detenido en las funciones principales de los mismos. Al final se presentaran los resultados obtenidos en estas mismas tablas para los equipos evaluados.

A continuación se presentaran descripciones de los equipos así como las principales imágenes ilustrativas de los mismos, para luego describir los apartados utilizados y finalmente hacer una breve comparación entre los dos equipos utilizados de los elementos evaluados previamente.

4.2 Fortinet.

Empresa fundada en California en el año 2000 por Kevin Xie fundador de la compañía Netscreen la cual posteriormente fue vendida a Juniper, dentro de su gama de equipos el más representativo es el FortiGate que no es más que el identificativo para el dispositivo UTM como tal; además cuentan con servidores de correo, generador de reportes y antivirus en formato de software. En la figura 4.1 se muestra el logo representativo de este fabricante.

Figura 4.1 Logo de Fortinet.

4.2.1 Aspectos generales.

La familia de seguridad FortiGate cuenta con tecnología acelerada ASIC, la cual incluye en su interior Firewall, Antivirus, IDS, IPS, VPN, Web Filtering, Antispam. Sus modelos (alrededor de 20) los agrupa en tres grandes secciones dependiendo de las capacidades de usuarios que soporta cada uno: SMB & SOHO (Small Median Bussines & Small Office Home Office), Enterprise y Large Enterprise & Service Providers.

Para los equipos Fortinet empezaremos por describir la estructura del core de estos, el punto central de los dispositivos es propietario en su totalidad, de hecho tanto la parte del hardware como la parte del software central son especiales para este tipo de equipos, el procesador llamado FortiASIC (Application-Specific Integrated Circuit) la cual es usada para la protección de redes en tiempo real ya que rompen el límite de procesamiento de contenidos gracias a su capacidad para procesar la gran cantidad de datos necesarios para analizar contenidos en tiempo real.

En cuanto al software de los equipos Fortinet , este es llamado FortiOS siendo la verdadera parte funcional que permite disfrutar de todas las bondades de este UTM en tiempo real, es

necesario aclarar que este sistema operativo es constantemente actualizado para dar una verdadera protección a la red involucrada. En este punto es necesario mencionar que la combinación de OS y el procesador, permiten la creación de dominios virtuales (vdoms) que no son más que segmentaciones lógicas de equipos dentro de un mismo equipo físico.[22] En la figura 4.2 se presenta la imagen de un procesador y las bondades del sistema operativo usados en equipos Fortinet.

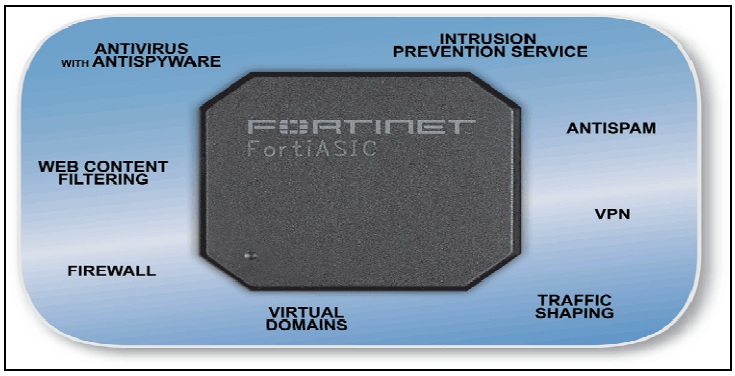


Figura 4.2 Ilustración de procesador y características de OS de equipos Fortinet

4.2.2 Técnicas utilizadas.

Como se menciono en capítulos anteriores, las licencias hoy en día son de gran importancia para mantener actualizado los niveles de seguridad de la red. Fortinet no es la excepción y pone al servicio de sus clientes la completa gama de licencias de seguridad dinámica, la cual dependiendo de la necesidad del cliente puede ser segmentada a los servicios que este último desee, sin embargo muchas veces suele ser más económico el adquirir el paquete completo de las mismas. La lista total de licencias incluye: Antivirus/Antisyware, Instrusion Proteccion, Web Filtering y AntiSpam.

En el caso de Fortinet, existen múltiples servidores de bases de datos a nivel mundial los cuales son consultados cuando se necesite una actualización de cualquiera de las protecciones antes mencionadas, presentando estos una especie de redundancia por si en algún momento no se tuviera acceso a alguno de ellos se pudiera conectar a cualquiera de los restantes. En la figura 4.3 se muestra un mapa con los distintos servidores de base de datos que Fortinet utiliza.

[22] http://www.fotinet.com, fuente consultada en junio 2008

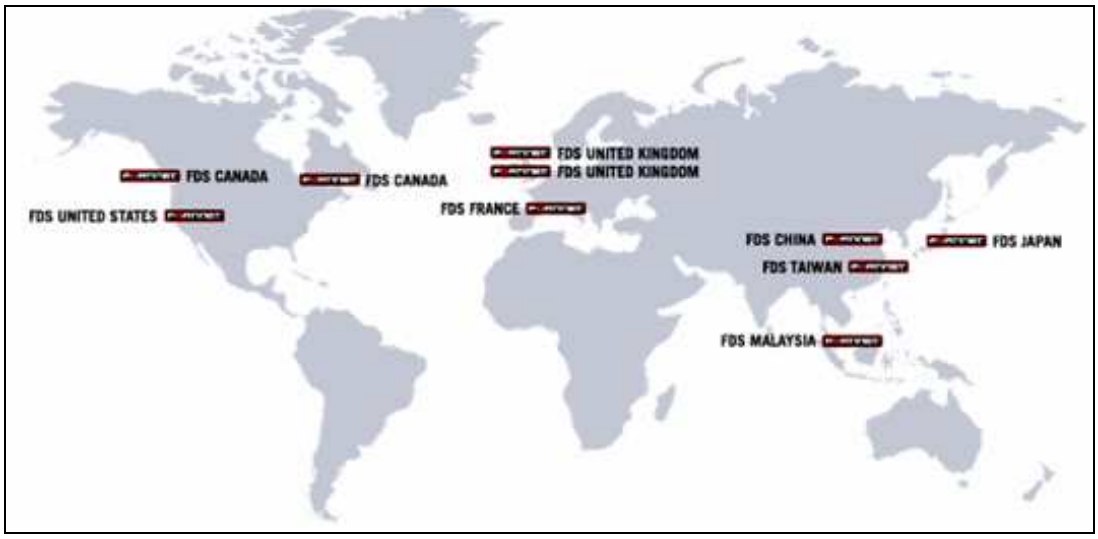


Figura 4.3 Servidores de bases de datos usados para actualizaciones de amenazas.

La identificación de amenazas requiere una alta capacidad de procesamiento lo cual está íntimamente relacionado con el número de usuarios que se necesite proteger, motivo por el cual cada procesador de cada modelo en específico va elevando su capacidad de acuerdo al número de usuarios que pueda soportar. En la figura 4.4 se muestra una grafica ilustrativa de lo antes mencionado, presentando al lado derecho las amenazas y su respectiva demanda al procesador en el lado izquierdo de la misma.

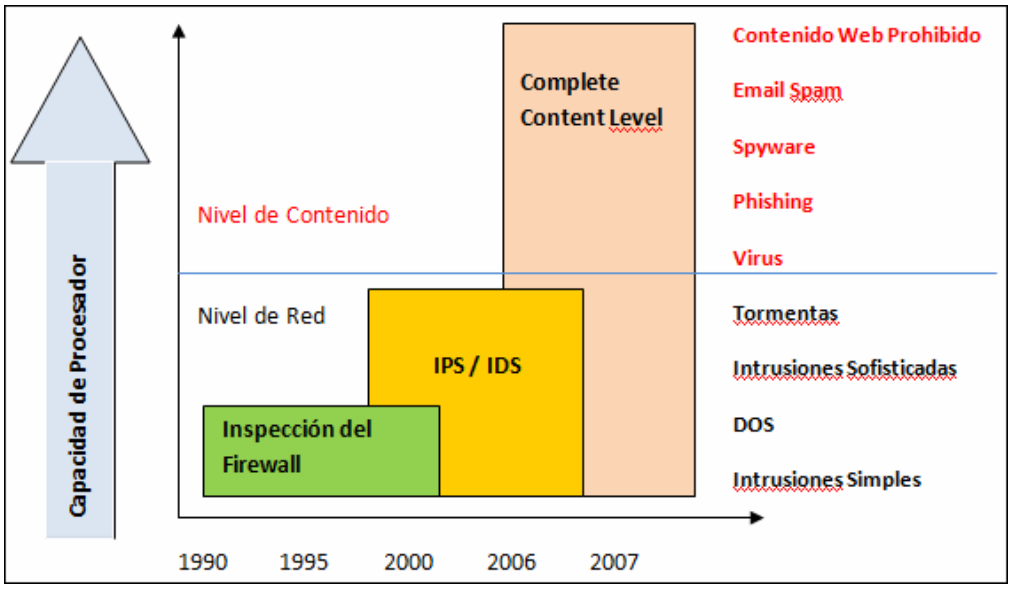


Figura 4.4 Demanda de procesador según la aplicación a identificar.

Este fabricante utiliza diferentes técnicas para la inspección de amenazas, entre ellas se tienen:

Stateful Firewall:	- Políticas de seguridad granular - Autenticación de usuarios - QoS
Antivirus:	- HTTP, FTP, SMTP, POP3, IMAP. - Firmas, actividades y métodos heurísticos.
IDS & IPS:	- Firmas, anomalías, inspección de actividades.
Antispam:	- Listas estáticas, bases de datos propietarias, RBL
Web Filtering:	- Listas estáticas, bases de datos propietarias
Encriptación:	- IPSec, SSL
Traffic Shaping:	- Prioridad de tráfico. - Tasas de de transferencias garantizadas y máximas.

En la figura 4.5 se muestra de forma grafica los módulos usados para la protección de amenazas.

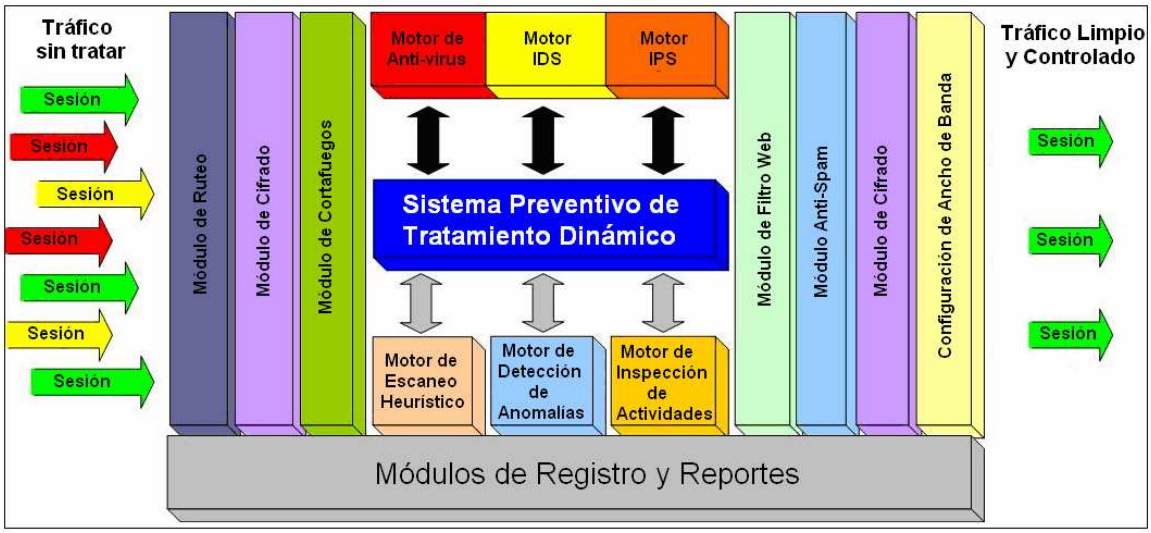


Figura 4.5 Ilustración de módulos usados para la inspección de amenazas.

Las técnicas usadas para la detección de amenazas son:

- Stateful Inspection.
- Application Inspection.
- Deep packet Inspection.
- Full Content Inspection
- Activity Inspection

En la figura 4.4 se muestran las capacidades de procesamiento requeridos para tipos de amenazas enfocadas a aplicaciones definidas, es para estas últimas que se utilizan las técnicas de Full Content y Activity Inspection. De las técnicas antes mencionadas únicamente las últimas dos no fueron descritas en capítulos anteriores, por lo que a continuación se hace un pequeño análisis de estas, que son usadas como técnicas de identificación de patrones de tráfico.

Las técnicas de Full Content Inspection y Activity Inspection constituyen la técnica denominada por el fabricante como Complete Content Protection, la cual consiste en descomponer o separa los paquetes de las tramas recibidas, con el fin de analizar la estructura completa y por separado de cada trama, permitiendo así analizar e identificar cada segmento para verificar si en el interior de este no se está intentando infiltrar algún trafico malicioso; luego de esto, la trama se vuele a ensamblar, por lo que si no hay anomalías en ella se permite el libre acceso a la red, de existir anomalías se colocan por separado las tramas tratando de realizar la limpieza de este tráfico, de no ser posible se procede a eliminar a estos paquetes o tramas infectados.

Los beneficios del procesador ASIC de Fortinet son usados en gran medida para proveer aceleración para los análisis de firmas, encriptación de tráfico y funcionalidades de SSL. Además son utilizadas técnicas de reensamblaje de paquetes por sesiones, inspecciones por firmas, e inspecciones heurísticas para lograr identificar el tipo de tráfico que se tiene presente en cada dispositivo.

El Sistema de Prevención de Amenazas Dinámicas (DTPS) de Fortinet es utilizado para aumentar la capacidad de detección de amenazas conocidas y desconocidas. Esta es usada en las secciones de Antivirus, IDS, IPS y módulos de firewall; sobre todo para identificar trafico malicioso que no cuenta con firmas definidas para su reconocimiento.

En la parte de detección heurística Fortinet la utiliza en gran medida para la parte de antivirus y antispam. Sin embargo la parte de escaneo de antivirus se incluyen: análisis de archivos, inspección de gusanos, análisis de tipos de archivos, inspección de firmas.

El segmento de IDS e IPS incluye herramientas como Stateful Inspection, reensamblamiento de contenido, inspección de protocolo de comunicación, inspección de

protocolo de comunicación e inspección de contenido. Todo esto con el fin de examinar e identificar todo el tráfico, generando el menor número de falsos positivos e identificar los ataques del día cero.

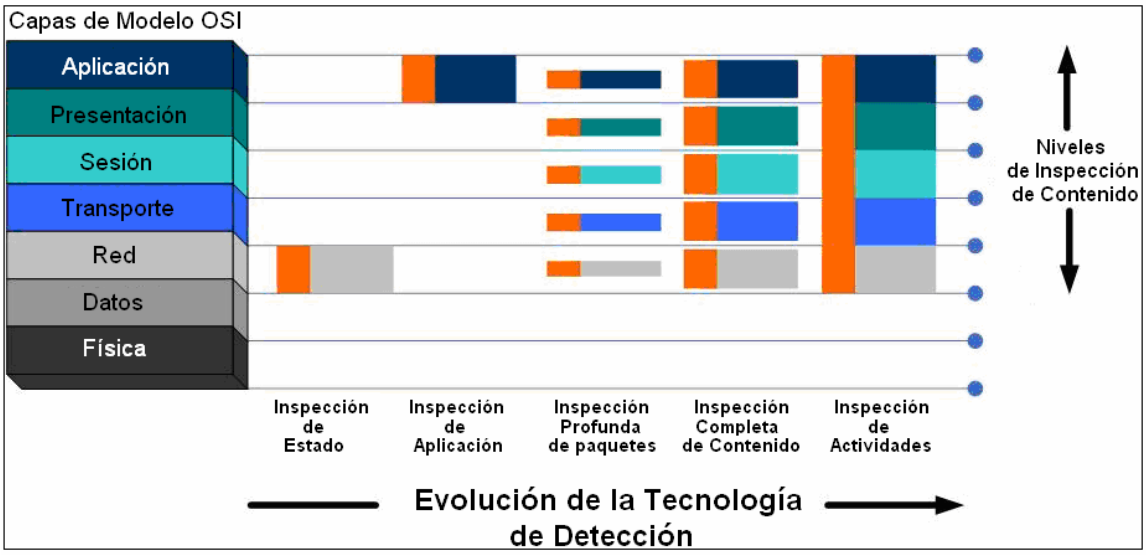


Figura 4.6 Ilustración de las tecnologías de detección de amenazas.

Todo lo anterior va enfocado a la utilización de la mejor técnica para la identificación de cada amenaza, el siguiente cuadro muestra una ilustración de cómo se clasifica y utilizan los métodos antes mencionados para ejemplos concretos, para esto se muestra un cuadro resumen en la tabla 4.2.

Amenaza	Ejemplo	Identificador
Intrusiones basadas en conexión	Ataques Telnet	Stateful Inspection
Ataques de protocolos	Inundacion SYN, Inundacion ICMP	Analisis de protocolos
Ataques de contenido de paquetes	Sobrecarga de buffer, tormentas	Deep packet inspection
Ataques de contenido de archivos	Virus, troyanos	Complete Content Protection
Amenaza de contenido de archivos	Contenido web inapropiado	Complete Content Protection

Tabla 4.2 Ilustración del uso de identificadores de amenazas.

4.2.3 Equipo Fortinet.

4.2.3.1 Elementos generales.

Se inicio con el conocimiento de la estructura del equipo, en la ventana principal se presentan datos importantes como el consumo de ancho de banda en determinado rango de tiempo y por cada interface en cuestión (1); por otro lado se puede observar gráficamente segmentados por IP los equipos que tienen establecidas más sesiones (2); también se presenta la utilización del procesador del equipo el cual según lo recomienda el fabricante no debe exceder el 75% en su funcionamiento normal (3); otro punto importante es el resumen de amenazas, spam, virus, transferencias de archivos por ftp, sesiones archivadas y correos, todos los que se visualizaron recientemente (4); así mismo se muestra un grafico con las interfaces del equipo haciendo referencia a las que en ese momento se están utilizando (5); además se tiene acceso a la información general del equipo como el IOS con el que se cuenta en ese momento o el tiempo que el equipo lleva funcionando (6); para terminar se puede acceder fácilmente a la consola de línea de comandos (CLI) desde el ambiente grafico algo realmente novedoso y útil en los equipos de seguridad (7). Una grafica de esta ilustración se presenta en la figura 4.7.

Figura 4.7 Imagen de la ventana principal de un equipo Fortinet.

El menú principal del equipo se presenta en forma de pestañas en la parte izquierda del mismo, desplegándose once categorías las cuales se subdividen en varios apartados cada una, pudiéndose dividir estos últimos en pestañas con el fin de poder acceder a partes más específicas de cada área. En la figura 4.8 se presenta una ilustración del menú principal con las siete categorías principales.

Figura 4.8 Ilustración de menú principal de Fortinet.

4.2.3.2 Descripción del menú principal y las sub categorías más importantes.

a) System

Esta categoría se subdivide en siete apartados más: Status, Network, DHCP, Config, Admin, Cerificates y Maintinance. La función de estas se presenta a continuación.

Status: Presenta la configuración inicial descrita anteriormente y la imagen mostrada en la figura 4.7.

Network: presenta tres pestañas dentro de ella Interface, Zone y Options, la primera de ellas da opción a configurar cada interface con su dirección IP respectiva, su máscara de red y sus protocolos de acceso HTTP, HTTPS, PING, SSH, TELNET y SNMP; se manera que se puede segmentar cada interfaz física con protocolos de acceso diferentes.

Es de hacer notar que el equipo no permite la configuración de dos interfaces físicas con el mismo segmento de red. La pestaña de Options permite configurar los DNS al equipo.

DHCP: como su nombre lo indica permite la configuración de esta función a cada interfaz por separado, asignando a cada interfaz rangos de IP definidos con la opción de asignar MAC address de equipos a IP's del segmento de red respectivos. De la misma manera por cada interfaz se tiene el agregado de configurar el acceso a equipos que generen el DHCP para cada interfaz.

Config: en este apartado se realiza la configuración de HA (High Avalability) con la cual se interconectan dos dispositivos UTM con el fin de generar balanceo de carga o proporcionar redundancia de equipos en la conexión. Por otro lado en este apartado se realiza la configuración de comunidades SNMP que permitan almacenar la generación de tráfico en cada interfaz en sistemas externos de registro de tráfico. Finalmente en la pestaña de operación se permite la configuración del equipo como un dispositivo capa tres es decir como ruteador o como dispositivo capa dos es decir como bridge, cabe mencionar que en esta ultima configuración el equipo se ve limitado en muchas de sus capacidades sin embargo pudiese llegar a ser necesaria dicha configuración en algún momento sobre todo cuando se necesita al equipo para funciones especificas que no impliquen las capacidades de ruteo.

Certificates: presenta el perfil del administrador, aquí se puede realizar la configuración de algún otro usuario con acceso diferente al del administrados que se quiera o se necesite generar en el equipo. De la misma manera se tiene acceso conexiones con dispositivos externos del mismo fabricante al equipo, entre ellos se puede realizar la interconexión con el FortiReporter o FortiAnalizer.

Maintenance: en esta parte se realiza el backup de la configuración del equipo, así mismo desde esta parte es posible cargar alguna configuración existente al equipo. Por otro lado se puede acceder a las licencias que se tienen activas, verificando la fecha de caducidad así como la fecha de la última actualización y configurar algunos parámetros de las mismas.

b) Router

Static: como su nombre lo indica, en esta parte es posible la configuración de rutas estáticas por cada interface física, pudiendo utilizar el parámetro de Distance que no es más que la prioridad otorgada a cada ruta, este parámetro es de gran importancia sobre

todo si se requiere de algún tipo de enlace redundante en cualquiera de las diferentes interfaces físicas.

Dinamic: en este apartado es posible realizar ruteo dinámico en interfaces físicas definidas, el dispositivo permite la configuración de cuatro protocolos: RIP v1 y v2, OSPF, BGP y Multicast.

Monitor: este apartado visualiza todas las rutas que el equipo está utilizando o que ha adquirido de alguna forma, presentando por cada ruta aprendida valores como la distancia, la métrica, el Gateway, la interfaz involucrada y el tiempo que tiene dicha ruta de haber sido aprendida por el dispositivo.

c) Firewall

Policy: este apartado es la parte medular de la operación del dispositivo UTM en su totalidad, ya que es aquí en donde se asocian los accesos, los usuarios, las IP's, las interfaces, los servicios y los perfiles configurados en los demás apartados del dispositivo necesarios para controlar el tráfico que circula en el dispositivo, si existiera alguno de los parámetros que únicamente ha sido configurado pero no se ha asociado a ninguna política no tendrá efecto alguno en el control de tráfico requerido.

Las políticas se configuran entre interfaces, siendo posible configurar la misma política para diferentes interfaces. De la misma manera las políticas tienen prioridad dependiendo de la secuencia que se desee otorgarles, es importante mencionar que estas inician las búsqueda de coincidencias desde la parte superior, desplazándose hacia abajo de no encontrar asociaciones validas en cada política de cada interface.

Address: en este segmento es posible agregar grupos de IP's en segmentos definidos con el nombre respectivo otorgado por el usuario, a estos grupos es posible también asociar la interfaz a la que se conectaran físicamente permitiendo así un mayor control de las IP validas por cada interface.

Service: se presentan todos los servicios identificados y registrados por el equipo con su puerto y el tipo de protocolo de comunicación que utiliza. De la misma manera es posible agregar nuevos servicios para aplicaciones definidas o requeridas por el cliente, siendo posible agregar estos servicios a grupos definidos para luego ser agregados a la política respectiva de la manera más efectiva.

Schedule: la versatilidad de estos dispositivos se extiende hasta la creación de horarios definidos para políticas en especial, estos equipos son capaces de crear la definición de estos horarios según la necesidad del cliente, dando la opción de crearlos una única vez,

por un único rango de tiempo definiendo año, mes, día, hora, minuto del inicio y fin de la política aplicar o siendo capaces de generando de manera recursiva los 7 días de la semana o un día de la semana en especial por un rango definido de tiempo.

Virtual IP: muchas veces es necesaria la creación de IP virtuales, estas son de mucha utilidad sobre todo cuando se desea realizar mapeo específicos de puertos en la red de una interfaz especifica hacia otra interfaz con segmento de red diferente. La creación de estas IP virtuales permiten definir el tipo de protocolo a utilizar (TCP o UDP) con los puertos respectivos, asi mismo permiten agregarse a servicios definidos.

Proteccion Profile: un valor de mucha importancia es el de filtro dinámico de contenido web, es aquí donde se configura el control de aplicaciones según el tipo de protocolos usados y páginas web dependiendo de su categorización en servidores propietarios del fabricante. La versatilidad de la categorización web permite bloquear páginas web según su contenido o simplemente almacenar el acceso a estos sitios. Es posible la creación de varios perfiles para luego ser aplicados en políticas específicas con usuarios, horarios y servicios definidos.

d) VPN

SSL: la creación y configuración de VPN SSL es posible realizarla desde este aquí, es importante mencionar que para que esta funcione se debe configurar parámetros fuera de este apartado para luego asociarlos a la política respectiva. Ofrece dos posibles métodos de conexiones el modo túnel que requiere de la configuración de un cliente remoto y el modo web-server que únicamente requiere un Navegador en el sitio remoto.

IPSEC: recomendado para conexiones remotas permanentes, requiere un cliente IPSEC en el otro extremo de la conexión, este puede ser otro dispositivo Fortinet o bien un cliente software, en este apartado es posible configurar más de una VPN entre ambos equipos con el fin de ser usadas para diferentes propósitos o como redundancia entre distintos proveedores.

PPTP: no tan usada con SSL o IPSEC por su nivel bajo de seguridad sin embargo este dispositivo ofrece la opción de configurar una VPN PPTP, la cual permite usar el dispositivo como servidor y que se conecten clientes remotos desde distintos puntos físicos.

e) User

Local: permite la creación de usuarios internos de la red en el equipo, que luego pueden ser asociados a aplicaciones específicas o diferentes perfiles.

Remote: utilizado para la autenticación de acceso de usuarios utilizando equipos externos a la red Fortinet, utilizando las capacidades de estos. Permite la interconexión del dispositivo con aplicaciones LDAP (Lightweight Directory Acceess Protocol), RADIUS (Remote Authentication and Dial-in UserService) y TACACS+ (Terminal Controller Access-Control System).

Windows AD: apartado utilizado para la interconexión del dispositivo con el autenticador de usuarios Active Directory de Windows, este segmento es capaz de conectarse a varios segmentos de AD para manejar diversos niveles o cantidades de usuario, en base a estos niveles se pueden aplicar políticas definidas para cada grupo, así se evita la creación de perfiles para usuarios directamente en el UTM, solo se realiza en el AD la instalación de FSAE (Fortinet Server Autentication Extension) para lograr la interconexión entre ambos dispositivos.

User Group: se utiliza para agrupar a los usuarios para aplicaciones VPN, autenticación de usuarios con recursos internos y/o externos o grupos de usuarios para perfiles definidos en el UTM.

Autentication: permite configurar los protocolos HTTP, HTTPS, FTP o telnet, que soportaran la autenticación de usuarios para los diversos aplicativos que la requieran; además en este punto es posible la configuración de certificados de seguridad definidos como SSL, IPSEC, o algún otro definido por el usuario.

f) Antivirus

File Filter: permite configurar perfiles de amenazas contra virus definidos, las cuales pueden variar entre la evaluación de aplicativos, correos electrónicos o archivos circulantes por el dispositivo. Por defecto viene configurado un perfil que evalúa todo el tráfico circulante por el dispositivo.

Quarentine: luego de haber identificado una posible amenaza (virus) se procede a mantener en cuarentena al archivo malicioso, es aquí donde se puede observar los detalles del archivo, la fecha y el tipo de amenaza detectada. Si este no pudiese ser limpiado se procederá a eliminarlo.

Config: en este apartado se pueden observar el listado de virus reconocido y para los cuales el dispositivo ofrece protección. Es de aclarar que este listado se auto-actualiza regularmente para ofrecer una mejor protección de seguridad. De la misma manera permite controlar el análisis de los virus categorizando las amenazas por aplicaciones y dándole al usuario la posibilidad de escanear o no escanear el tráfico circulante por este equipo.

g) Intrusion Protection:

Signature: en este apartado se pueden observar las firmas que el dispositivo puede identificar, el protocolo usado, la categorización de cada firma, el sistema operativo que utiliza y el estatus de cada una. Es importante aclarar que por defecto el equipo únicamente identifica el trafico permitiendo el paso de todo el a menos que se indique lo contrario. De la misma manera da la opción de agregar alguna firma que el usuario crea conveniente o que necesite identificar.

IPS Sensor: luego de haber identificado el tráfico circulante por el dispositivo, es necesario restringir o permitir el paso de tráfico en específico. Esto es fácil de controlar ya que en este apartado están categorizadas por defecto algunas las firmas como las de servidor de correo, las de cliente estándar, las de permitir el acceso de todas; de la misma manera el cliente puede crear el perfil que considere necesario.

DoS Sensor: un ataque muy frecuente y sobretodo muy peligroso es el DoS, este apartado permite la configuración de protecciones exclusivas para esta anomalía, permitiendo crear varios perfiles los cuales pueden enfocarse en IP, interfaces o políticas definidas.

h) Web Filter

Content Block: el bloqueo o acceso de páginas web además de utilizar el método dinámico otorgado con las licencias anuales, se puede realizar en base a expresiones regulares o a palabras definidas en diferentes idiomas las cuales se localizan a la página web a la cual se requiere accesar, las cuales las define el usuario en base a sus necesidades.

URL Filter: otra opción a los métodos antes mencionados de permitir o bloquear acceso a páginas web es el de controlarlo en base a direcciones web especificas.

i) Antispam

Banned Word: de la misma manera como se bloquean páginas web en forma estática es posible realizar el bloqueo de spam en base a palabras definidas por el usuario. Estas palabras se pueden agrupar en grupos definidos para facilitar al momento de aplicar esta restricción a usuarios o interfaces definidas.

Black/White List: en caso de contar con un servidor de correo conectado directamente al equipo o ser este externo a la red interna es muy útil este apartado ya que permite restringir el análisis de correo para IP o cuentas de correo en específico; por otro lado de la misma manera permite la clasificación de alguna IP como generadora de spam para que todo el trafico proveniente de este sea catalogado como tal.

j) IM, P2P & VoIP

Statistics: como su nombre lo indica en este segmento se encuentran las estadísticas de los aplicativos IM, P2P y VoIP.

User: el equipo permite obtener la visualización de las cuentas de MSN y P2P logeadas recientemente, además permite controlar las sesiones de MSN en base a las cuentas logeadas.

k) Log & Report

Log Config: aquí se configura el equipo que recibirá los logs captados por el UTM, por si solo el dispositivo en su memoria solo guarda los logs recientes en cada apartado, el fabricante recomienda interconectarse con otro dispositivo que el fabrica llamado Forti-Analyzer, el cual genera reportes de gran calidad y bastante detallados. Otra opción viable es la interconexión con un syslog a manera de almacenar los logs del equipo. De la misma manera es posible la configuración de generación de correos a medida se generan alarmas de gran importancia. Por otro lado también es posible la configuración de los parámetros que realmente le interesan monitorear al usuario del equipo.

Log Acces: permite verificar los logs almacenados ya sean estos almacenados en el dispositivo o en equipos remotos.

Content Archive: se utiliza únicamente para verificar los datos almacenados en el Forti-Analyzer, estos pueden verificarse en 5 categorías Web, E-Mail, FTP, IM y VoIP.

Report Config: utilizado para verificar el reporte generado por los equipos remotos a partir de los logs enviados desde él.

Report Acces: ilustración grafica de los protocolos y anchos de banda utilizados por el dispositivo en los últimos días.

4.2.3.3 Parámetros Básicos.

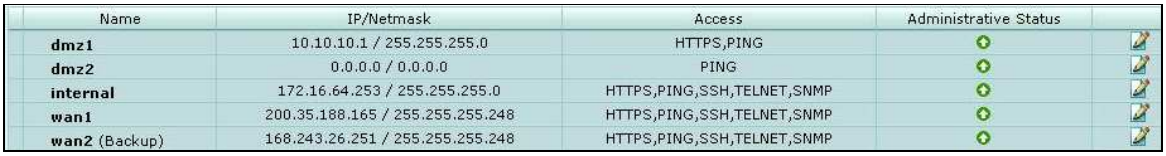
Las pruebas realizadas consistieron en la comprobación de aspectos básicos del equipo ya que por el poco tiempo que este dispositivo fue concedido, solamente se pudieron realizar pruebas de nivel básico, estas se realizaron con la ayuda de los manuales que el mismo fabricante proporciona para cada apartado específico.

La configuración general: configuración de rutas estáticas, configuración de redundancia de ISP, registro y activación de licencias, verificación de parámetros de página principal.

El equipo en un inicio se entrego sin configuración alguna más que las configuraciones que por defecto el equipo posee, como los perfiles de protección antivirus, antispam, IPS y el filtrado de contenido web básico.

Debido a lo anterior, se requería iniciar con la configuración de los parámetros básicos para obtener navegación en el equipo. Se configuraron en las interfaces WAN las IP publicas otorgadas por los ISP dejando una de ellas como salida principal y la otra como ruta redundante, definiendo los protocolos por medio de los cuales se podría accesar a dicha interfaz; a continuación se realizo la configuración de las interfaces LAN y las rutas estáticas utilizadas por los usuarios de la red interna que hasta el momento funcionaban con otro dispositivo de similares características. La configuración de las interfaces del dispositivo se muestra en la figura 4.9

Las pruebas realizadas con la conmutación de ambas interfaces WAN fueron satisfactorias presentando caídas de tres pruebas de ping a la hora de la conmutación física realizándolas desde dentro de la red hacia afuera, siendo estos tiempos bastante aceptables.



Name	IP/Netmask	Access	Administrative Status	
dmz1	10.10.10.1 / 255.255.255.0	HTTPS,PING		
dmz2	0.0.0.0 / 0.0.0.0	PING		
internal	172.16.64.253 / 255.255.255.0	HTTPS,PING,SSH,TELNET,SNMP		
wan1	200.35.188.165 / 255.255.255.248	HTTPS,PING,SSH,TELNET,SNMP		
wan2 (Backup)	168.243.26.251 / 255.255.255.248	HTTPS,PING,SSH,TELNET,SNMP		

Figura 4.9 Ilustración de configuración de las interfaces

Luego se procedió a configurar para los usuarios, alrededor de veinte personas, el listado de perfiles específicos tomando en cuenta que se establecen IP fijas para cada usuario, en un

inicio se configuro el mismo perfil para todos los usuarios limitando el acceso a sitios pornográficos, con el objetivo de comprobar la información de la página principal y la utilización de la capacidad de procesador. Se procedió a tomar la imagen mostrada en la figura 4.8, la cual se describe detalladamente a continuación.

Ilustración de las interfaces físicas del dispositivo, se presenta en color verde las interfaces conectadas, en color gris las no conectadas y en el extremo derecho se presenta las posibles interconexiones con dispositivos externos del mismo fabricante que permiten un mejor desempeño en conjunto de las posibilidades que este UTM ofrece por sí solo. Como la generación de reportes (FortiAnalyzer) o el manejo en conjunto de varios de estos dispositivos interconectados entre sí (FortiManager). La ilustración de lo antes mencionado se presenta en la figura 4.10.

Figura 4.10 Descripción Física del equipo.

Como se ilustra en la figura 4.11; en la página principal se presenta un resumen de las principales estadísticas de registro del equipo y pueden ser accesibles con más detalle con solo seleccionar el link verde ubicado en el lado derecho de cada uno.

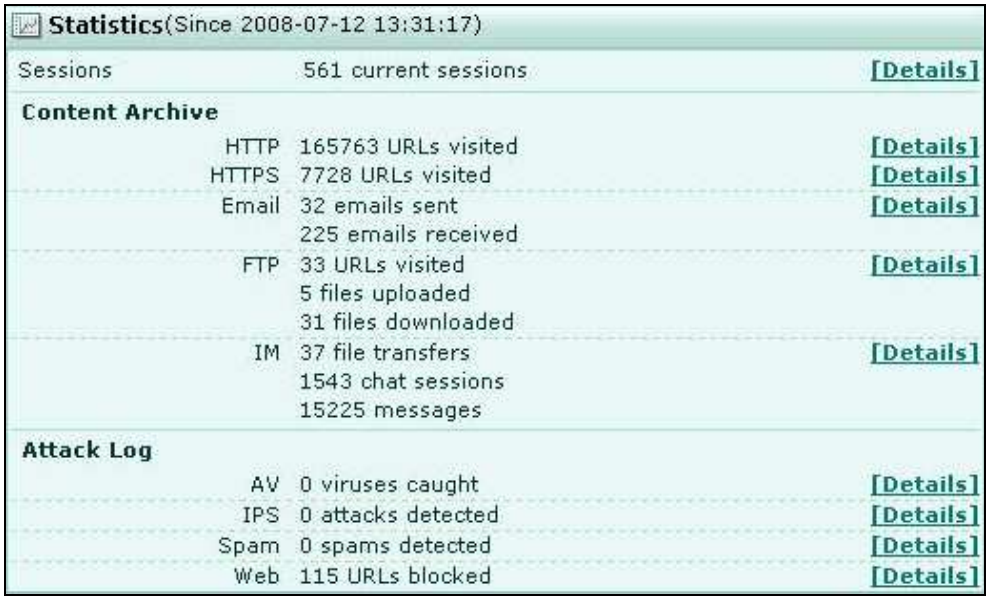


Figura 4.11 Ilustración de las estadísticas.

En la figura 4.12 se presenta la imagen de las sesiones establecidas en el equipo presentándose la IP de la LAN así como la IP externa con la cual está establecida la sesión.

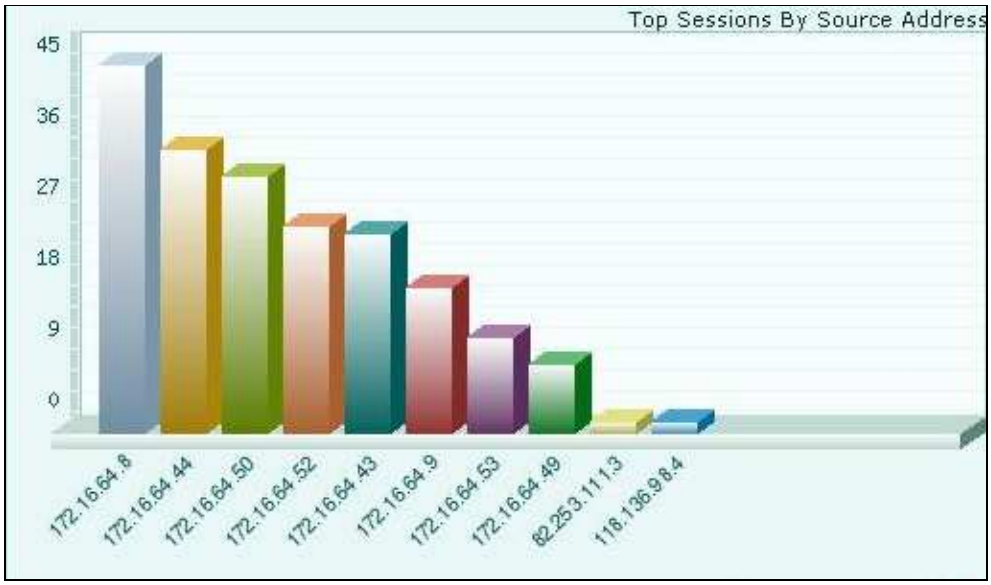


Figura 4.12 Ilustración de sesiones establecidas.

De la misma manera se presenta el acceso a la consola del equipo desde la interfaz grafica, la utilización del microprocesador y la memoria del equipo, estas dos últimas no deben sobrepasar el 75% de su uso para un desempeño optimo según recomendaciones del fabricante. Lo anterior se ilustra en la figura 4.13.

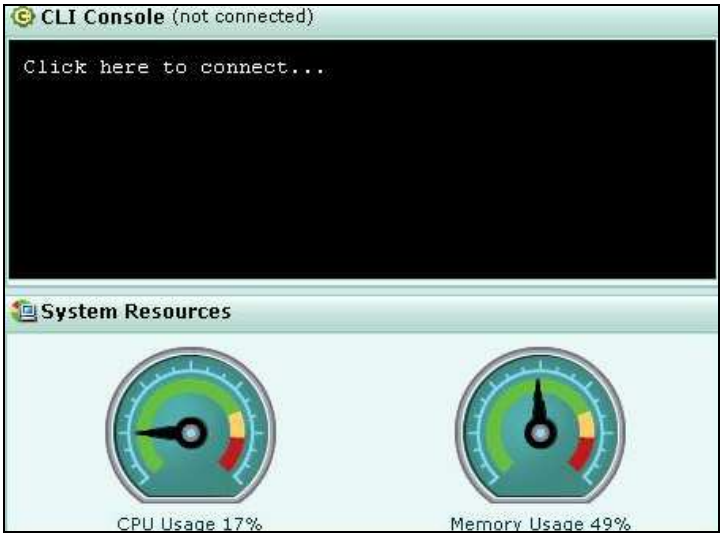


Figura 4.13 Ilustración de CLI y la utilización de recursos del equipo.

Se presenta además la ilustración del desempeño del equipo que el mismo dispositivo ofrece en la figura 4.14, la imagen mostrada ilustra el desempeño de la interface interna, pero igual puede ser visto desde cualquier interface del equipo. En donde la grafica verde presenta el tráfico de salida de la interface y el tráfico rojo el tráfico de ingreso a la misma.

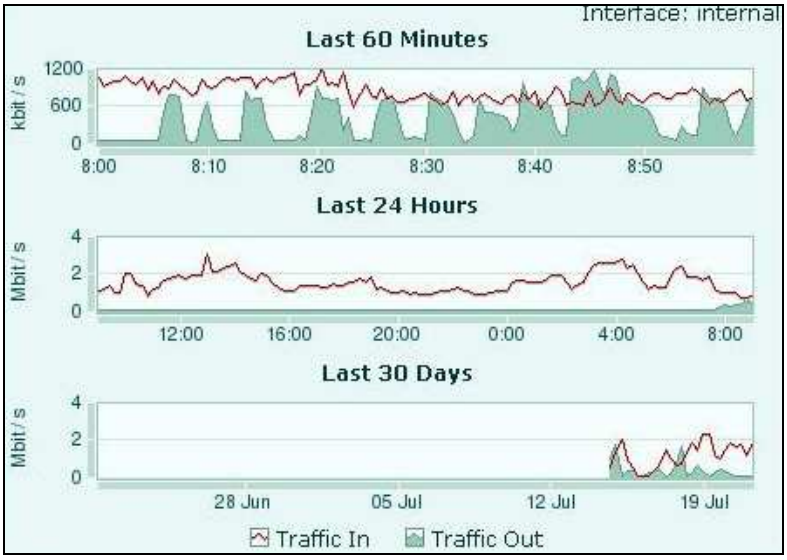


Figura 4.14 Ilustración del desempeño del equipo.

Luego de la configuración de usuarios y los parámetros básicos de navegación se tomo la imagen 4.15 desde la ubicación: *Firewall / Policy*, en donde se ven reflejadas las configuraciones iníciales de las políticas configuradas en un primer momento. Como se puede observar la configuración de políticas en este equipo se realizan de acuerdo a las interfaces involucradas, en estas mismas se puede aplicar controles en base a horarios, servicios y asignarles perfiles definidos a cada una.

Status	ID	Source	Destination	Schedule	Service	Profile	Action
internal -> wan1 (4)							
☑	1	all	all	always	ANY	unfiltered	ACCEPT
internal -> wan2(Backup) (1)							
☑	2	all	all	always	ANY		ACCEPT
wan2(Backup) -> internal (2)							
☑	3	all	all	always	ANY		ACCEPT
wan1 -> internal (3)							
☑	4	all	all	always	ANY		ACCEPT

Figura 4.15 Ilustración de las políticas iníciales.

De la misma manera se realizo la configuración de servidores DHCP en una interface, siendo posible asignar servidores a cada interfaz física y asignar la IP según sea la MAC address del equipo solicitante. De igual forma se realizo la configuración de una comunidad SNMP, la cual enviaba todo el tráfico proveniente del equipo a un administrador de tráfico instalado en la red interna local. En la figura 4.16 y 4.17 se muestra la ilustración de ambos puntos descritos anteriormente.

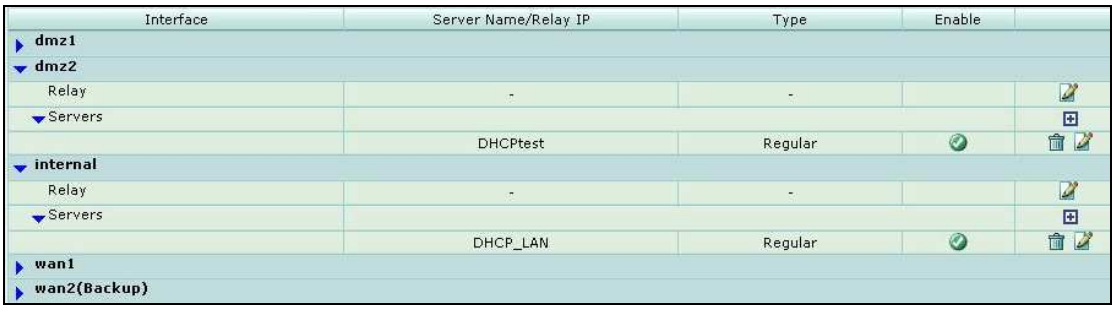


Figura 4.16 Configuracion de DHCP

Figura 4.17 Configuración de DHCP y comunidad SNMP utilizados

4.2.3.4 Configuración de VPN

a) VPN SSL

En la parte de creación de VPN se realizo la configuración de las modalidades IPSEC y SSL. Para esto fue necesario desplazarse hacia el segmento de *VPN / SSL* en el menú del equipo, como primer paso se procedió a la configuración de la VPN SSL, debido a que sería de mayor utilidad en el ambiente a evaluar ya que se necesitaban configurar accesos remotos para clientes con movilidad y que se necesitarían conectar por rangos cortos de tiempo. En la figura 4.18 se presenta la imagen de la pantalla de configuración con el rango

a utilizar para accesar desde la VPN, permitiendo cifrar en tres técnicas diferentes. De la misma manera aquí se define si se requerirá de un cliente definido de SSL en el otro extremo o se realizara por acceso web, es decir un browser. Esta última modalidad fue la que se configuro en las pruebas realizadas.

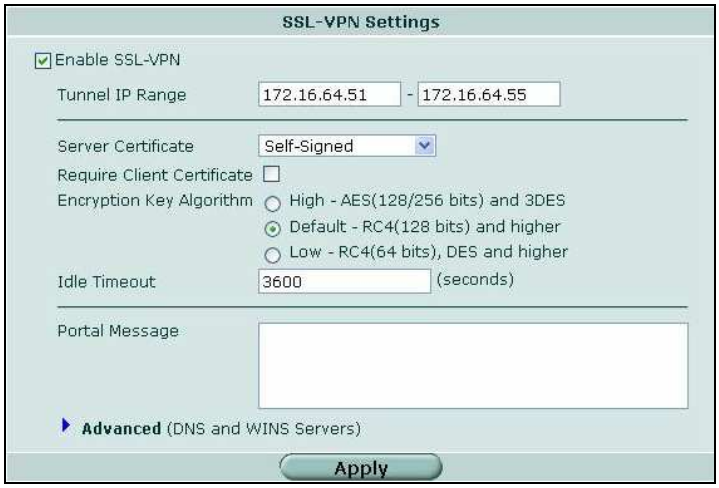


Figura 4.18 Configuración de VPN SSL

Es de aclarar que para finalizar la configuración de una VPN es necesario además de lo antes mencionado, definir un usuario con su respectivo password que puede ser autenticado por el mismo equipo o por equipos externos (LDAP, RADIUS o TACACS+), además de configurar un usuario en el equipo que se agregara junto con lo antes mencionado a una política definida para que pueda ser aplicado por el dispositivo. En la figura 4.19 se muestra la imagen del acceso otorgado a través de la VPN una vez autenticado el acceso al equipo.

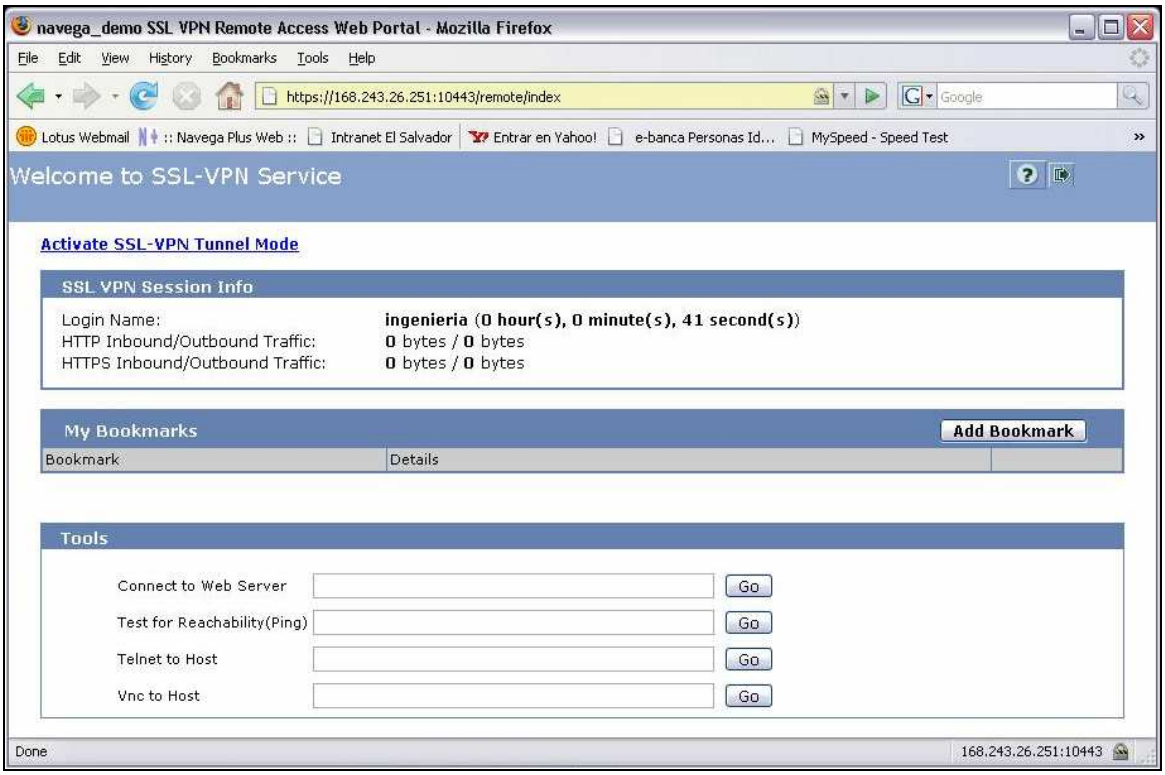


Figura 4.19 Ilustración de acceso remoto usando VPN SSL

Una vez logrado el acceso el posible acceder a un servidor web, realizar pruebas de ping, ejecutar telnet o utilizar un servidor VNC instalado en una PC con IP dentro del rango definido a la hora de la creación de la VPN. Se ejecutaron 3 pruebas de las 4 posibles, dejando de lado la primera mencionada, teniendo resultados satisfactorios en las 3 realizadas. Sin duda la más útil es la de acceder vía VNC ya que prácticamente se logra trabajar como si se estuviese desde el interior de la red accesada. En la figura 4.20 se presenta la imagen lograda a partir del acceso vía VNC.

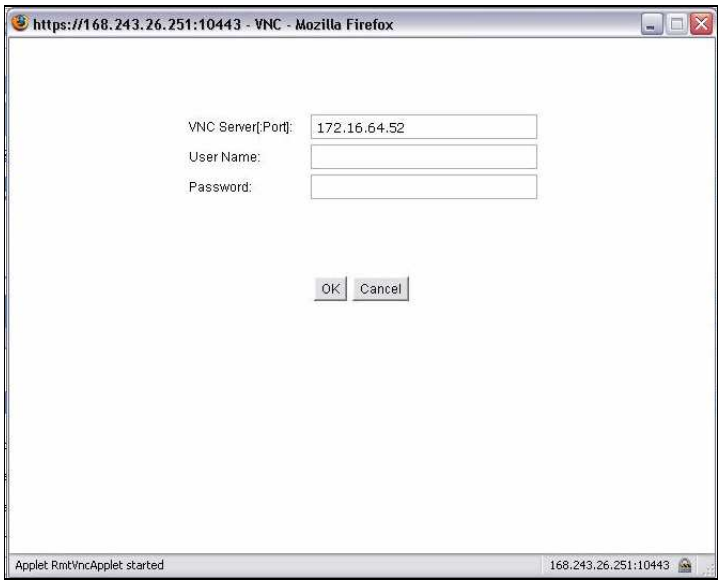


Figura 4.20 Ilustración del acceso VNC a la red interna usando VPN SSL.

b) VPN IPSEC

En lo que respecta a la VPN IPSEC, existen diversas modalidades de realizar la configuración, esta puede ser utilizando dos o más equipos capaces de realizar VPN IPSEC o bien utilizando un cliente en versión software para mantener activa o permanente la conexión. Para el caso se utilizo un cliente IPSEC proporcionado por el mismo fabricante del UTM.

La configuración de esta VPN es un tanto más complicada que la de SSL, sin embargo está diseñada para que una vez configurada se mantenga activa la conexión permanentemente. Lo más recomendable según el fabricante es generar la conexión entre dispositivos similares ya que por la multiplicidad de parámetros a configurar pudiese llegar a ser un tanto complicado el establecer la VPN entre dispositivos diferentes.

La configuración en el dispositivo se realiza en dos fases, la configuración se realiza desde la ubicación *VPN / IPSEC* el cual se ilustra en la figura 4.21 en donde se realiza buena parte de la configuración como definir las IP's que conformaran la VPN y el tipo de encriptación a utilizar. En la fase 2 se define el Gateway remoto, el nombre del túnel y la IP del host remoto con el cual se comunicara, fuera de este apartado se necesita configurar una ruta estática que indique "el camino" para acceder al segmento de red remoto que se estará comunicando entre la VPN. Finalmente se asocia la información antes creada a una política definida, donde se especifican las interfaces involucradas así como se pudiera indicar algún horario específico para su operatividad o el acceso de algún servicio en especial.

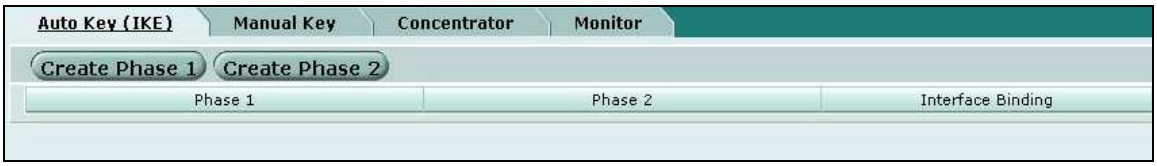


Figura 4.21 Configuración de VPN IPSEC

Luego de la finalización de la configuración de la VPN en el dispositivo, se necesitaría de una configuración similar en el otro extremo ya sea este un UTM o un cliente software como en este caso se realizo. Se utilizo la versión software del equipo que el mismo fabricante proporciona, el nombre de este aplicativo es Forticlient.

Este puede ser instalado como un firewall de usuario final o instalarse únicamente con las aplicaciones a utilizar, por si mismo este aplicativo posee cinco módulos que se pudieran instalar en una PC, estos son Firewall, Web Filter, Antivirus, Antispam y VPN. Para nuestras pruebas únicamente se instalo este ultimo modulo.

Una vez instalado el aplicativo, el cual se muestra en la figura 4.22, se procede a la configuración de la VPN. Se inicia con la configuración de la sesión VPN, luego se coloca la IP del Host remoto con el cual se establecerá la comunicación, la red remota a la que se accederá y el método de autenticación que debe ser el mismo que el usado en el Fortigate junto con la calve (preshared key) con esto ya está finalizada la configuración, solo resta establecer la comunicación entre ambos puntos. En la figura 4.23 se muestra la ilustración de la comunicación establecida desde ambos puntos involucrados.

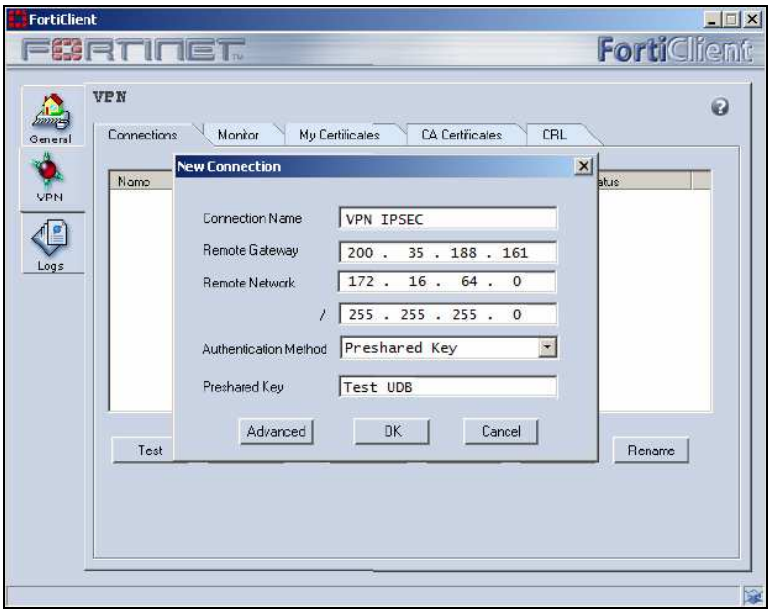


Figura 4.22 Cliente IPSec utilizado

Figura 4.23 Comunicación establecida desde ambos dispositivos.

4.2.3.5 Configuración de Perfiles

Con respecto a la configuración de perfiles, esta se puede realizar de varias formas, la más utilizada por su simplicidad es la de agrupación de IP por sus funciones o necesidades laborales, desde el apartado de *Firewall / Address* simplemente basta con definir los rangos de IP's a agrupar para luego nombrarlos y agregarlos a políticas especificas. La ilustración de esto se presenta en la figura 4.24, en donde se agregaron únicamente tres agrupaciones de IP, sin embargo estas pueden ser un número mayor.

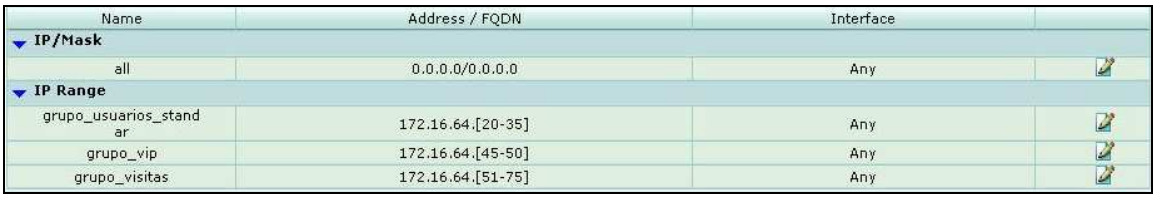


Figura 4.24 Ilustración de agrupaciones de IP.

De la misma manera, la creación de perfiles es posible realizarla generando autenticación de usuarios esta puede ser desde el mismo equipo o desde dispositivos externos con los cuales el dispositivo es capaz de interconectarse. En las pruebas se realizaron creaciones de usuarios definidos, estos al logearse pueden ser asociados a políticas definidas, es un método un tanto más difícil de evadir para los usuarios finales ya que no importa desde que equipo terminal intente navegar o acceder a alguna aplicación, su perfil será siempre el mismo. Para realizar esta configuración se debe de ubicar en el apartado de *User / Local*, la ilustración del resultado de esta configuración se presenta en la figura 4.25.

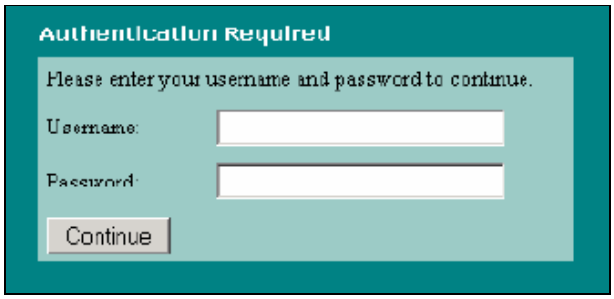


Figura 4.25 Ilustración de la autenticación configurada en equipo UTM.

De igual manera la autenticación de usuarios puede ser configurada desde dispositivos externos, con el fin de aprovechar la utilidad de las bases de datos que han sido creadas específicamente para este fin. Para lo cual se requiere instalar en el servidor externo una aplicación que permita la comunicación entre ambos dispositivos, esta aplicación es llamada FSAE (Fortinet Server Authentication Extension) y es provista por el fabricante del UTM. Las configuraciones de estas autenticaciones externas se realizan desde el segmento *User / Remote,* en donde se permite la comunicación con servidores LDAP, Radius y Tacacs+.

En las pruebas se configuro la comunicación entre el Active Directory de Windows y el UTM, esto se realiza desde el apartado *User / Windows AD* primero se inicio con la instalación en el servidor de FSAE. Una vez finalizada la instalación se coloco la IP del agente que contiene la información del AD utilizando el puerto por defecto 8002. Esto se ilustra en la figura 4.26. Una vez detectadas las cuentas del AD podemos indicarle que cuentas se necesitan monitorear del Fotinet y cuáles no, se recomienda monitorear todas las cuentas para tener control completo en el UTM.

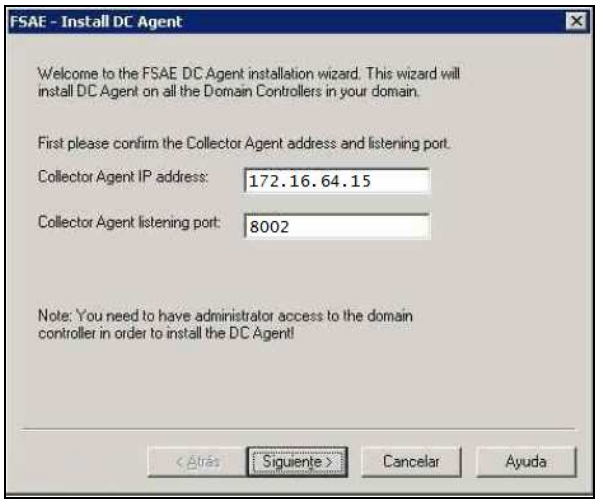


Figura 4.26 Configuración de FSAE en el AD

Una vez finalizada la configuración en el AD, se configuro en el UTM la parte restante; esta consiste en colocar la IP, el identificador del AD configurado y la contraseña del mismo. Luego de lo anterior debe observase en el UTM el listado de usuarios proveniente del AD. Se muestra la imagen de la prueba realizada en la figura 4.27. Solamente quedaría pendiente la asociación de un grupo a este AD para luego poder asignarlo y administrarlo bajo cualquier política que se desea.

Figura 4.27 Listado del AD.

Los perfiles también se pueden controlar en base a horarios (HH/MM/SS), días de semana o simplemente fechas, estas pueden ser recurrentes o aplicarse en una sola fecha específica. Para realizar esta configuración se debe acceder a *Firewall / Schedule*. Estos horarios luego pueden ser aplicados a una o más políticas según sea la necesidad, en la figura 4.28 se muestra la ilustración de la configuración realizada, se definió un horario recurrente utilizado para permitir el acceso al MSN (lunch) a un grupo específico de personal y luego un horario creado para aplicarse una única vez (MSN).

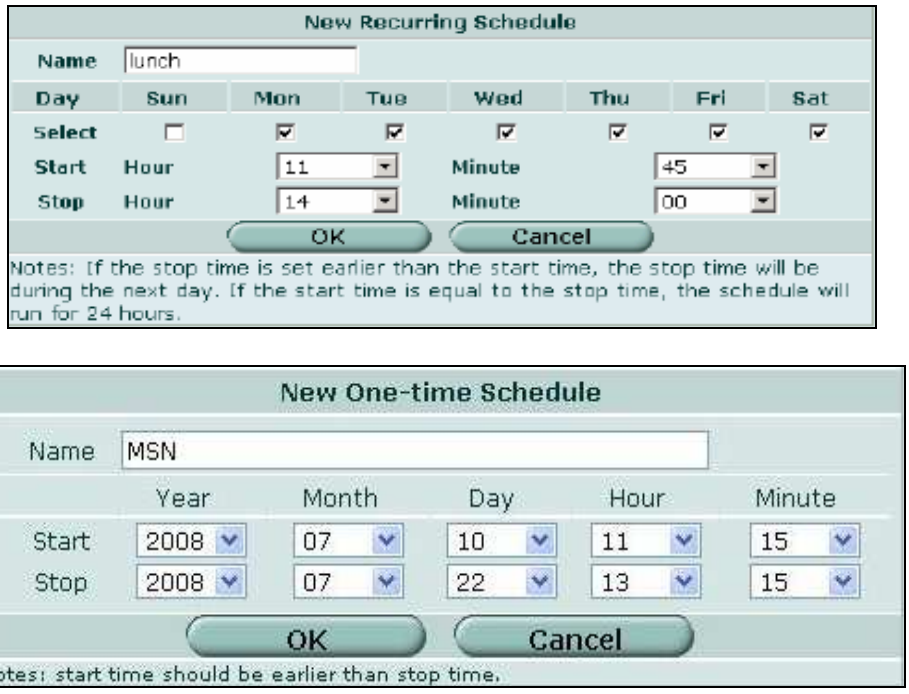


Figura 4.28 Modalidades de horarios configurados.

4.2.3.6 Filtrado de contenido web

4.2.3.6.1 Filtrado web estático

El filtrado de páginas web además de realizarse de manera dinámica también es posible controlarlo de manera estática, aunque la efectividad de esta actividad no es tan grande como el filtrado dinámico, muchas veces se necesita alguna de estas opciones. La configuración estática se puede realizar de dos formas ya sea definiendo expresiones regulares o definiendo URL especificas.

Para definir la frase se requiere accesar a *Web Filter / Content Block* en donde se pueden agrupar varias palabras o frases para tener un mejor manejo en la aplicación de políticas, estos listados bien pueden ser usados para restringir o permitir palabras específicas en diferentes idiomas como inglés, español, francés o chino. En la figura 4.29 se presenta la imagen de la configuración realizada, mientras que en la figura 4.30 se muestra una página web bloqueada utilizando esta configuración, en donde el mensaje mostrado puede ser modificado mediante lenguaje HTML.

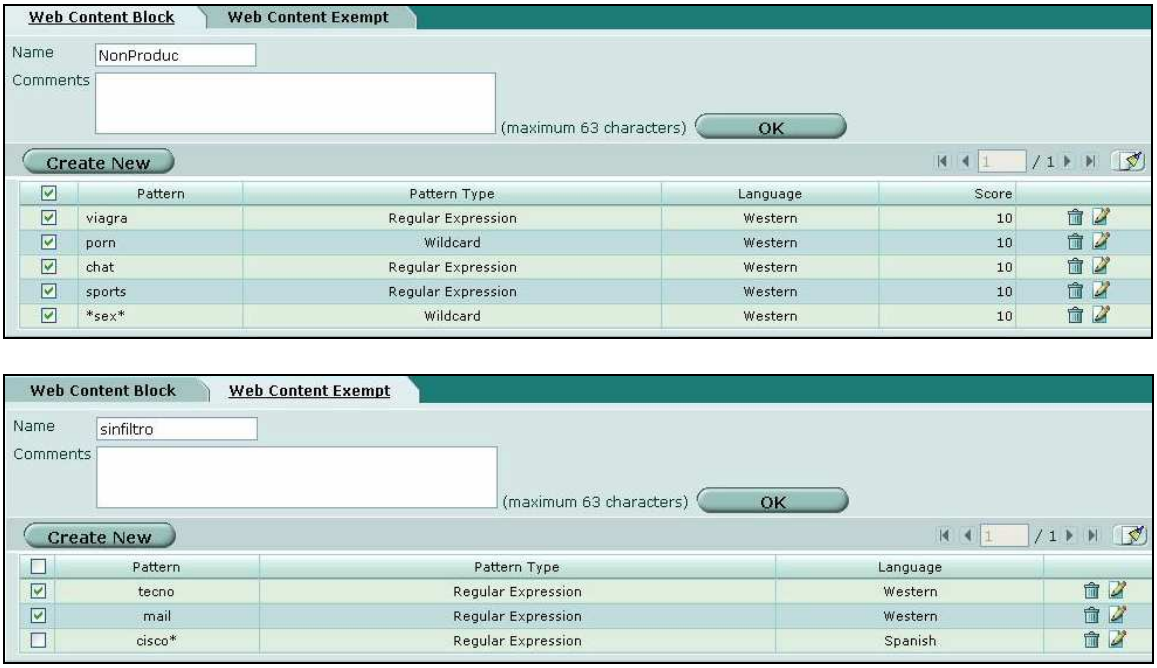


Figura 4.29 Listas creadas para boquear y permitir palabras definidas en páginas web

Figura 4.30 Bloqueo de pagina web al aplicar las políticas de la figura anterior.

Por otro lado, se puede realizar el control a páginas web específicas usando las URL para permitir o denegar acceso a estas. La configuración se realiza en el apartado *Web Filter / URL*. La imagen mostrada en la figura 4.31 es la de la configuración utilizada y la de la imagen 4.32 es la de la imagen resultante después de aplicar dicha configuración y posterior a realizar las modificaciones en lenguaje HTML para este apartado.

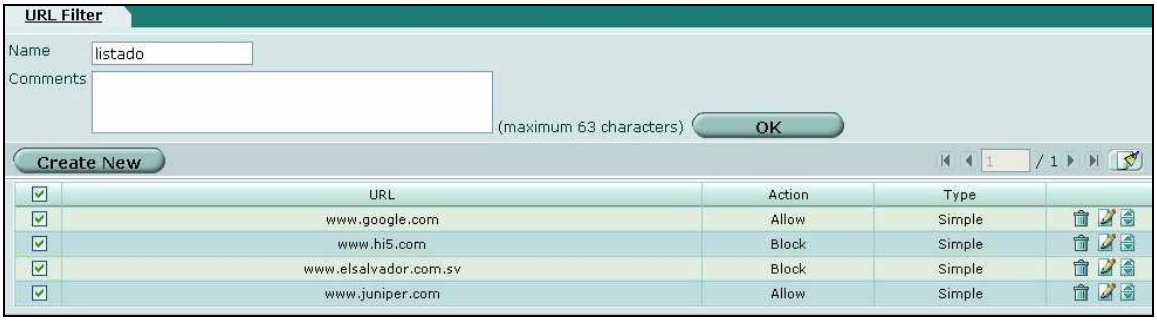


Figura 4.31 Configuración utilizada para bloquear/permitir URL definidas

Figura 4.32 Bloqueo de pagina web utilizando el filtro de URL.

Estos métodos de configuración estática se utilizan como complementos del control dinámico, su uso es para palabras más puntuales o URL que en el filtro dinámico se verían afectadas, por ejemplo si se quisiera restringir solamente el acceso a la página web de un banco en especifico, es mucho más sencillo bloquear todas las paginas financieras en el control dinámico y permitir la URL usando el control estático de la institución necesitada.

4.2.3.6.2 Filtrado web dinámico

Este tipo de filtrado se realiza en el apartado *Firewall / Proteccion Profile* donde es posible definir el tipo de tráfico o aplicaciones que se desean controlar, además es aquí donde se utiliza el control de tráfico dinámico llamado FortiGuard Web Filtering, el cual permite controlar tráfico en base a categorizaciones de páginas web, una imagen de estas categorizaciones se presentan en la figura 4.33. En donde se observan las categorizaciones antes mencionadas pudiendo permitirse o denegarse el acceso a páginas web dentro de esta categoría o simplemente registrar las páginas web accesadas en el equipo, sin embargo dentro de ellas también es posible ser más granular aun, por ejemplo en la categoría de Controversial se encuentran sub categorías como Contenido para Adultos, Desnudez, Vocabulario Agresivo entre otras, las cuales pueden ser también tratadas de manera independiente.

En la imagen presentada se observa que la categoría Controversial no está ni permitida ni bloqueada en su totalidad, es porque se tratan a las subcategorias independientemente como se mencionaba en el párrafo anterior, es decir algunas son permitidas y otras son bloqueadas, esto dependerá mucho de las necesidades que el usuario requiera.

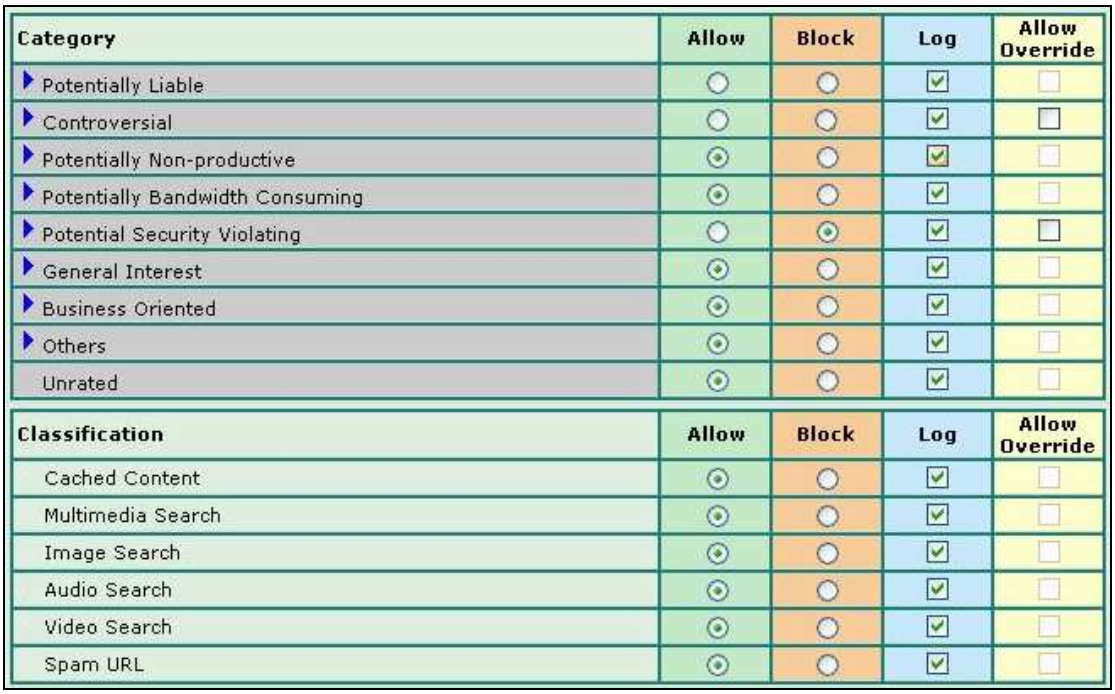


Figura 4.33 Ilustración del filtro de contenido dinámico.

Para este caso se realizo una prueba con una página web utilizando la categorización mostrada en la figura 4.33, tratando de acceder a una página con contenido para adultos, el resultado se presenta en la figura 4.34, en donde se observa el bloqueo de la misma y se explica de la misma manera en el mensaje presentado la razón por la que fue bloqueada, así mismo existe un link que puede servir al usuario para hacerla petición de reconsiderar la re-categorización de la pagina si este así lo cree conveniente.

De la misma manera se acceso a otra página web en donde se publicaban anuncios con contenido del mismo tipo, la imagen capturada se presenta en la figura 4.35, en donde se observa que el segmento bloqueado únicamente es donde se presenta esta publicidad con contenido para adultos.

Figura 4.34 Pagina web bloqueada de manera dinámica.

Figura 4.35 Publicidad para adultos bloqueada en una página web.

Finalmente se puede observar tanto el filtro web dinámico como estático, se realizan de diferente manera y con diferentes objetivos, sin embargo estas configuraciones se complementan entre sí con el fin de tener una mayor área de acción y hacer más versátil al equipo mismo, en efecto en el apartado del contenido web dinámico, existe la posibilidad de agregar las listas creadas en el apartado estático a un perfil definido con el objetivo de unificar o aplicar de una manera más sencilla los perfiles creados ya sean estáticos o dinámicos a usuarios o IP's definidas.

Aplicar esta interconexión siempre se realiza desde la parte de configuración dinámica, es decir desde *Firewall / Protection Profile*, únicamente se ubica el apartado nombrado como Web Filtering que está ubicado justo arriba de FortiGuard Web Filtering, en donde en la imagen de esta configuración que se muestra en la figura 4.36, hace referencia a las listas creadas en el apartado de filtrado web estático y mostradas en las figuras 4.29 y 4.31.

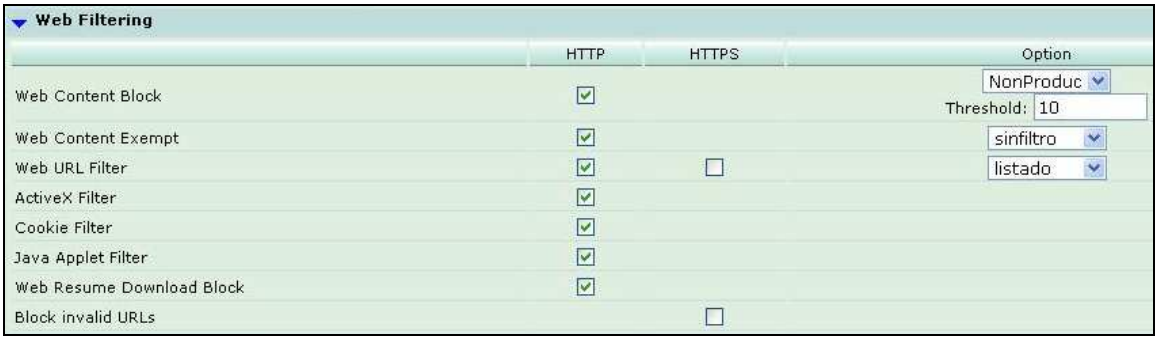


Figura 4.36 Filtrado web estático aplicado junto al filtrado web dinámico.

4.2.3.7 IM&P2P

4.2.3.7.1 IM

En el caso de IM y P2P se realizaron pruebas con ambas aplicaciones por separado. Se inicio con los aplicativos IM, en el apartado de *Firewall / Proteccion Profile* mostrado en la figura 4.37 en donde estas aplicaciones IM es posible guardar registro, bloquearlas por completo, bloquear el paso de archivos entre ellas, bloquear el audio e inspeccionar en puertos no comunes, como se observa se controlan los IM más usados AOL, ICQ, Hotmail y Yahoo.

Figura 4.37 Configuración de control sobre IM.

El control de páginas web usadas para el logeo de IM que es muchas veces el método más eficiente que los usuarios utilizan para evadir este tipo de control se pueden controlar desde el FortiGuard Web Filtering. Una imagen de esta limitación de transferencia de archivos aplicada se presenta en la figura 4.38, estos controles pueden ser configurados con diferentes perfiles para un mejor control del mismo. Sin embargo existe otro apartado que por la misma naturaleza del aplicativo ofrece valiosas herramientas extras para poder controlar el tráfico de este origen.

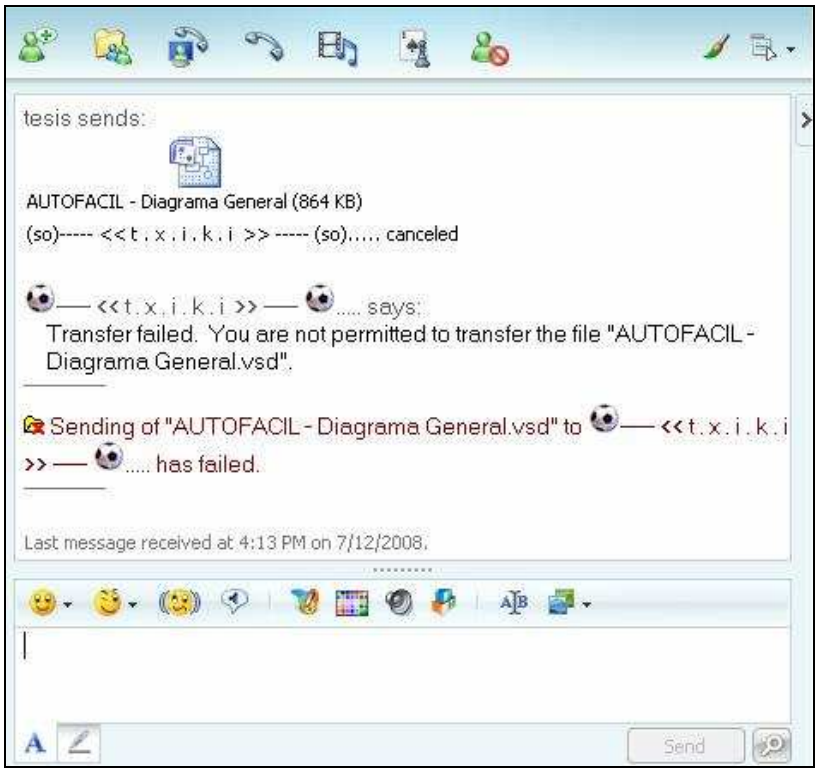


Figura 4.38 Ilustración del bloqueo de archivos a través del IM

El otro apartado mencionado en el párrafo anterior se refiere a la ubicación accesible desde *IM&P2P / User* en donde se pueden observar las cuentas de IM registradas, con esto se puede dar acceso o restringir el mismo a cuentas definidas de usuarios, haciendo aun más efectivo el acceso de los mismos, que si lo combinamos con el filtro dinámico de web Messenger, nos da un amplio margen de acción pero sobretodo de granularidad con este tipo de tráfico que es considerado complicado de identificar por la forma de operar del mismo.

En la figura 4.39 se presenta la imagen de la configuración y los datos registrados en la prueba realizada, en donde como se puede observar, se logean todas las cuentas que se han registrado desde un cliente de IM definido no importando si las cuentas son de diferentes servidores de IM, así mismo en la figura 4.40 se presenta la imagen del manejo directo de cuentas de IM que se puede realizar en este UTM.

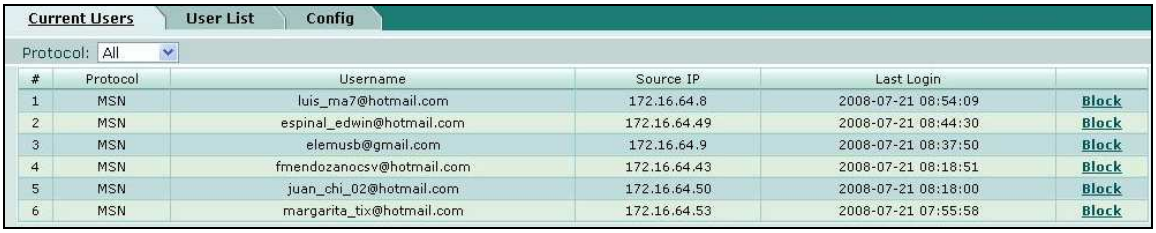


Figura 4.39 Imagen del registro de cuentas web.

Figura 4.40 Manejo de cuentas individuales de IM

Una limitante observada en este equipo, es que la aplicación de IM de Google Talk no es controlada por el mismo, a pesar que se negó el acceso a todas las aplicaciones IM esta aplicación en especial si pudo accederse sin ningún problema, quizá en futuras versiones de IOS esto sea corregido pero por el momento no es posible realizar dicho control.

4.2.3.7.2 P2P

Para el caso de P2P, se cuenta con el apartado de Firewall / Proteccion Profile en donde se tiene la opción de permitir, denegar o limitar el acceso para los aplicativos más comunes de este tipo de tráfico: BitTorrent, eDonkey, Gnutella, KaZaa, Skype y otros que han sido desarrollado a partir de algunos de estos como por ejemplo eMule que está basado en eDonkey.

La primera prueba que se realizo fue la de bloquear el acceso a este tipo de aplicativos, esta fue satisfactoria en su totalidad, al menos para los aplicativos que si es capaz de controlar y para versiones que dependan directamente de ellas.

Luego se utilizo la configuración de limitar el tráfico para las aplicaciones posibles, se instalo un P2P para efectos de prueba este fue limitado en sus tasas de comunicaciones, se utilizo eMule para realizar las mediciones, como se puede observar en la figura 4.41 la tasa de transferencia fue limitada a 15 KBytes, que es lo que se ve reflejado en la grafica proveniente del sistema de monitoreo utilizado, figura 4.42.

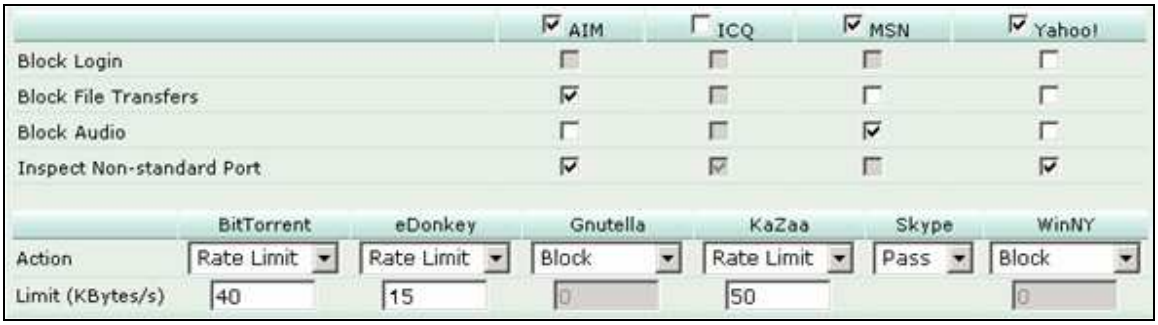


Figura 4.41 Imagen del tipo de manejo al tráfico P2P

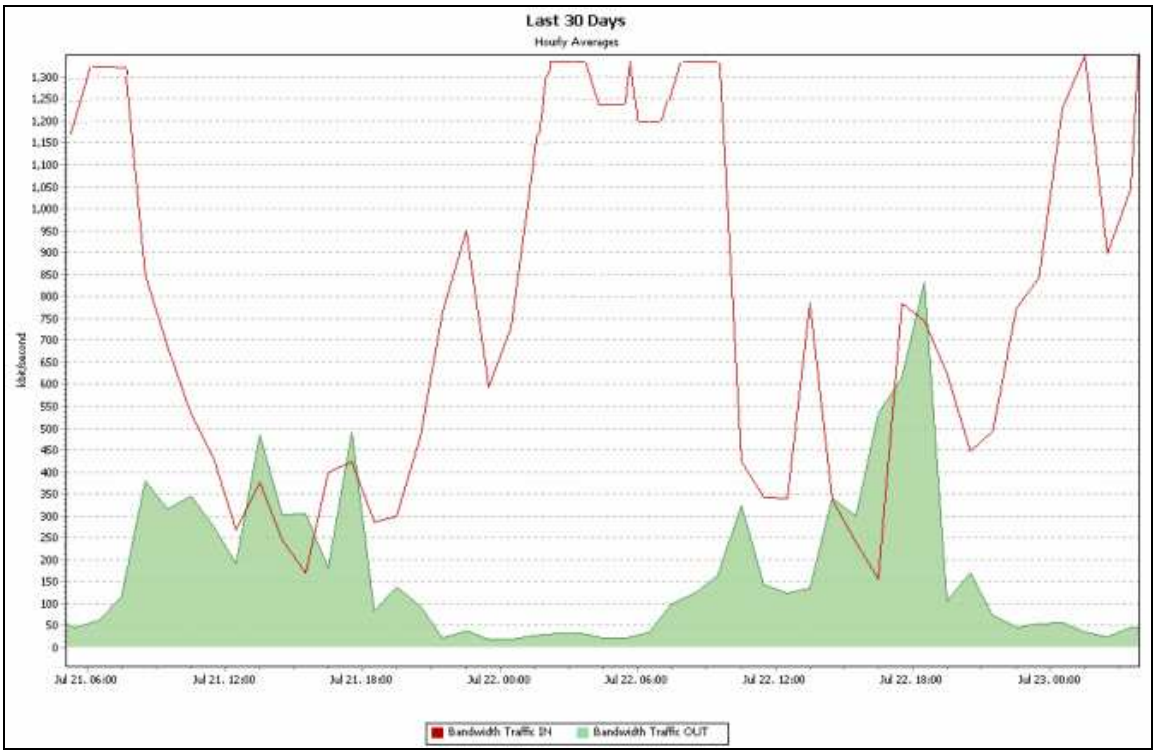


Figura 4.42 Tasa de transferencia limitada de eMule.

4.2.3.8 IPS

Para los sistemas IPS, se consulta el apartado *Instrusion Proteccion / Signature* donde se observan todas las firmas reconocidas y evaluadas por el dispositivo, sin embargo estas no implican que al reconocerse se bloqueen los protocolos identificados, de hecho el usuario debe indicar que trafico según el reconocimiento será bloqueado. Los protocolos identificados según el número de puerto y las firmas establecidas que el equipo reconoce se presentan en la figura 4.42.

Protocols	Ports
Back Orifice	Auto
DCE RPC	135, 1026
DNS	53
FTP	21
H323	1720
HTTP	Auto
Instant Messaging	Auto
IMAP	143
LDAP	389
MSSQL	1433
NetBIOS	139, 445
Peer-to-Peer	Auto
POP3	110
Protocol (L3/4) Analyser	Auto
RADIUS	1812,1813
Sun RPC	111, 32771
SIP	Auto
SMTP	25
SNMP	161, 162
SSH	Auto
SSL	Auto
TCP Reassembler	Auto
TFN DoS	Auto

Figura 4.42 Protocolos identificados por el equipo

Por defecto el equipo trae configurados perfiles de protección contra intrusos ya que resulta un tanto complicado establecer perfiles tomando en cuenta el elevado número de firmas disponibles. Estos perfiles según el nombre nos indican el nivel de seguridad que cada uno contiene facilitándonos el aplicarlo a las políticas respectivas. La ilustración de dichos perfiles se presenta en la figura 4.43.

Name	Comments	
all_default	all predefined signatures with default setting	
all_default_pass	all predefined signatures with PASS action	
protect_client	protect against client-side vulnerabilities	
protect_email_server	protect against EMail server-side vulnerabilities	
protect_http_server	protect against HTTP server-side vulnerabilities	

Figura 4.43 Perfiles configurados por defecto en el dispositivo.

Por otro lado es importante mencionar que en base a las firmas que el equipo posee, el usuario puede crear sus perfiles de protección contra ataques definidos o identificadores para aplicaciones que se utilizan o que pudieran servir para identificar algún tipo de trafico que por defecto no se encuentra registrado o que el equipo no controla por sí mismo, por ejemplo para otros tipo de IM o P2P que no son considerados en apartados anteriores, una vez identificados el usuario es capaz de negar el acceso a dichas aplicaciones.

Otro punto importante es el bloqueo de DoS que por defecto el equipo trae configurado, la frecuencia con que estos ataques afectan los sistemas informáticos han llevado a que se trate de manera especial a este tipo de ataque. En el segmento *Instrusion Proteccion / DoS* el equipo trae configurados un par de perfiles que limitan los ataques DoS, estos pueden ser modificados o eliminados por el usuario, sin embargo se recomienda aplicarlos en las políticas de todos los usuarios. En la figura 4.44 se presenta la ilustración de los perfiles configurados contra los ataques DoS.

Figura 4.44 Perfiles configurados por defecto contra el DoS

Una vez configurados los puntos anteriores se hace necesario el aplicar estos grupos IPS creados a un perfil para luego aplicarlo a una política; es por esto que se debe recurrir a el apartado *Firewall / Protection Profile* y aplicarse en el apartado de IPS el perfil deseado. En la figura 4.45 se presenta la imagen utilizada en el perfil creado.

Figura 4.45 Aplicación de grupo IPS en perfil de protección.

4.2.3.9 Antivirus

La sección de antivirus es accesible desde la ubicación *Anti Virus / File Filter* en este apartado el equipo trae por defecto un listado contra los virus más comunes, el cual puede ser aplicado en las políticas que se crean convenientes, en su totalidad la identificación detección de estos archivos se realiza de manera dinámica. Solo se permite que el usuario pueda crear listas específicas de firmas antivirus que requiera especial atención por el tipo de tráfico o de aplicaciones que se pudieran llegar a manejar en la red, dando mayor énfasis en algún tipo de estudio definido. La ilustración de esta configuración se observa en la figura 4.46.

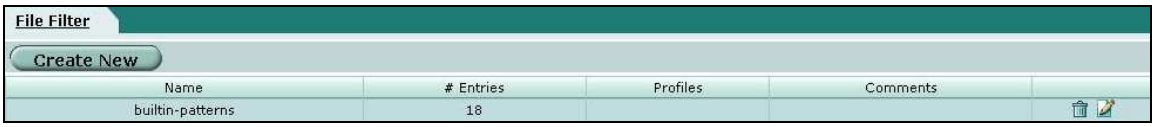


Figura 4.46 Configuración de listas Antivirus.

Si algún archivo o aplicación se encontrara infectada, esta se mostraría en el apartado de la cuarentena, que es accesible desde la ubicación *Anti Virus / Quarantine*. De la misma manera se puede observar el listado de virus que el equipo es capaz de identificar en la ubicación *Anti Virus / Config*.

Por otro lado, luego de haber creado el grupo adecuado o el usuario decidirse a utilizar el grupo que el equipo trae por defecto, se procede a aplicar a un perfil de protección en especial, esto se logra desde la ubicación *Firewall / Protection Profile*. En donde es posible configurar el análisis de archivos provenientes de páginas web, servidores FTP, correo electrónico (IMAP, POP3 y SMTP), IM y servidores de noticias en línea (NNTP).

La otra opción que ofrece el dispositivo en este mismo apartado es limitar la longitud de los archivos que circularan por el equipo, así como la posibilidad de agregar para el análisis de los correos de salida firmas definidas. En la figura 4.47 se presenta la ilustración de los controles aplicados a un perfil definido.

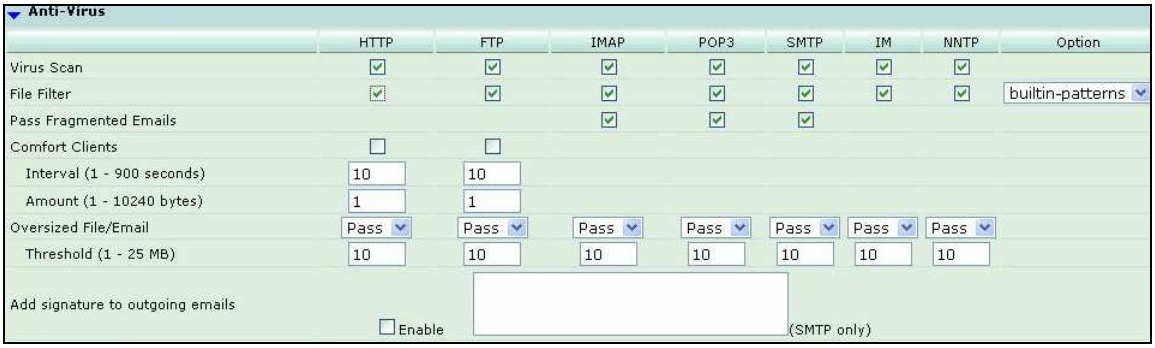


Figura 4.47 Aplicación de filtros antivirus

4.2.3.10 AntiSpam

Este apartado además de identificar de manera dinámica este tipo de trafico malicioso, permite la creación de grupos de palabras que requieran especial atención en el análisis, las cuales el cliente las puede agregar según sea necesario a las políticas definidas para cada usuario o grupos de usuarios las ocasiones que considere necesarias, esto se puede

configurar en diferentes idiomas; lo anterior es posible realizarlo desde el apartado *AntiSpam / Banned Word*, el cual se ilustra en la figura 4.48.

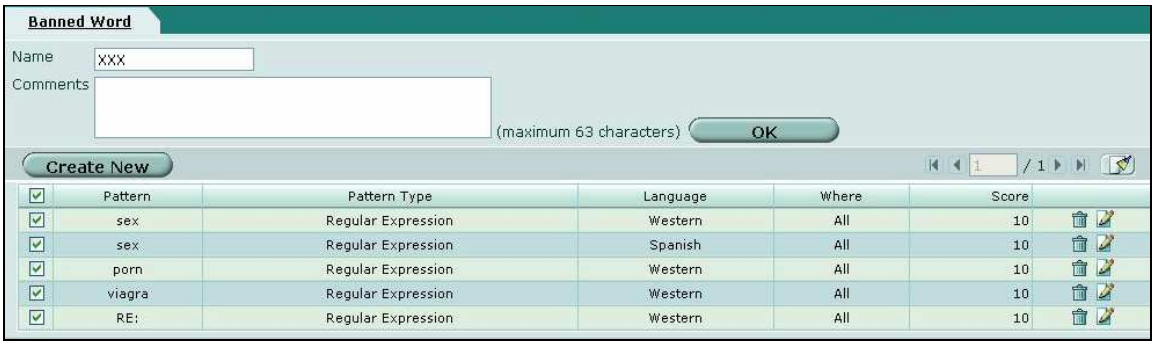


Figura 4.48 Listado de palabras creadas para la detección de spam

La configuración de la imagen anterior puede ser usada en dado caso, no se detecte algún correo spam por el equipo y se requiera de una configuración con una palabra específica para que este sea detectado. De la misma manera si se detectara alguna IP como generadora de spam, esta puede ser bloqueada de manera estática; lo mismo sucede si alguna IP es de nuestra total confianza y sabemos que de ella no podría venir ningún correo malicioso, esta IP se puede exonerar del análisis respectivo; similar control se puede tener si se define una cuenta de correo especifica.

En todos los casos anteriores, se pudiese realizar esto para quitarle carga al procesador encargado de realizar estos análisis y así darle mayor agilidad al proceso de identificar el tráfico anómalo. Una configuración que se utilizo se presenta en la figura 4.49.

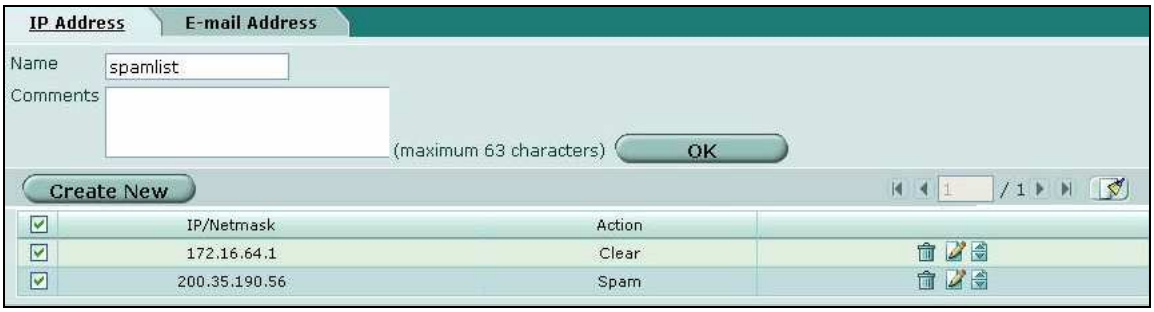


Figura 4.49 White/Black IP list

La asociación de estos grupos requiere se apliquen en una política, para ello se accede al apartado *Firewall / Protection Profile* en donde se permite controlar el tráfico malicioso en

los correos entrantes y salientes, además es posible configurar la protección de manera estática utilizando palabras definidas como expresiones regulares o analizando IP definidas, para el caso se muestra la asociación del grupo creado en la figura 5.48 en el perfil final utilizado. En la figura 4.50 se muestra el apartado que permite esta configuración.

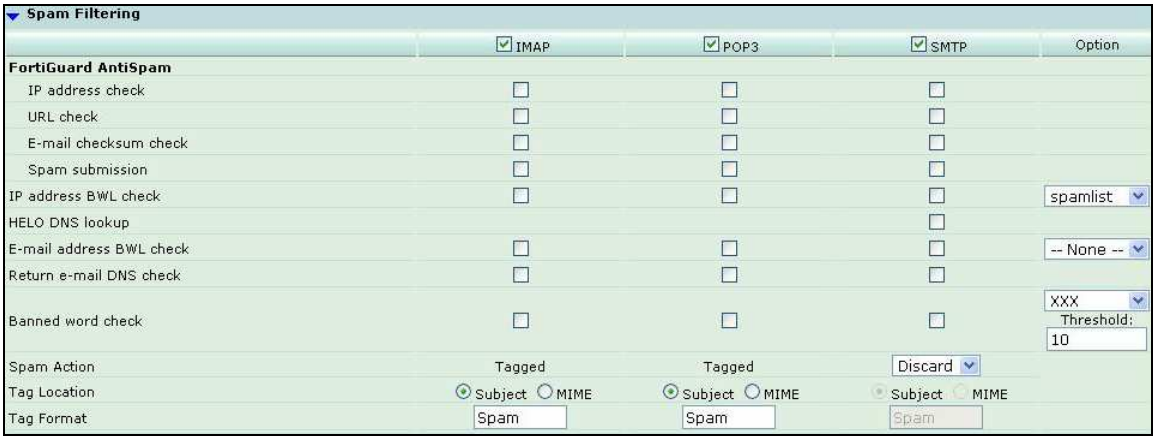


Figura 4.50 Asociación de grupos creados en perfiles de protección.

4.2.3.11 Reportes

Este segmento está limitado en el equipo si se considera como un equipo generador de reportes a este dispositivo. Tiene capacidad de almacenar logs por un corto tiempo, sin embargo no es lo suficiente como para generar algún tipo de registro que pudiese ser realmente útil en un periodo de tiempo determinado, sin embargo para contrarrestar este punto, tiene la ventaja de poder interconectarse con muchos equipos comúnmente usados para almacenar los logs que el captura, sin embargo si se quisiera aprovechar al máximo las capacidades de este equipo para generar reportes se pudiera interconectar con otro dispositivo de este mismo fabricante.

Las pruebas únicamente se realizaron con el Fortigate, en él se pudieron configurar los parámetros requeridos para almacenar en el mismo dispositivo los logs; para ello se requirió indicar estos datos en el apartado Log & *Report / Log Config*, lo cual es mostrado en la figura 4.51.

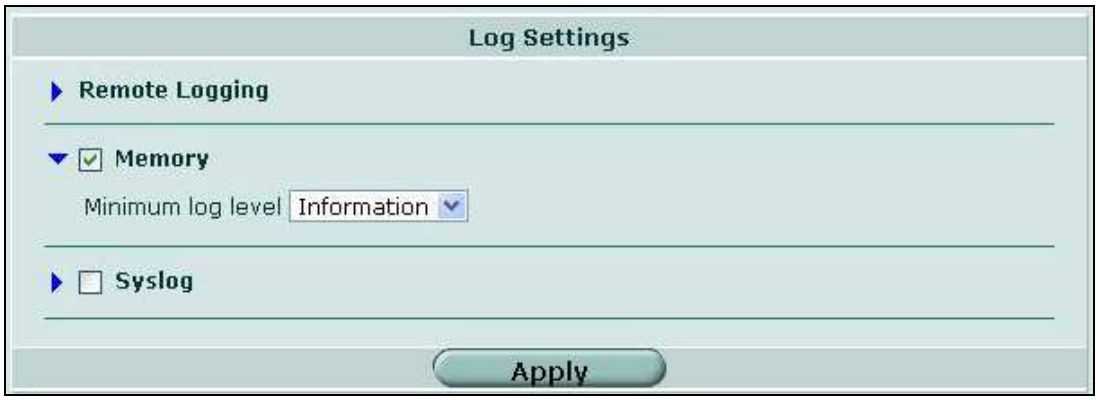


Figura 4.51 Configuración de almacenamiento de logs.

De la misma manera es posible indicarle el tipo de logs que queremos que almacene, esto se logra desde el mismo apartado y se muestra en la figura 4.52.

Figura 4.52 Logs que se requiere sean almacenados

Finalmente, luego de las configuraciones necesarias para que los logs sean almacenados en el equipo, se muestran los resultados de estos, en la figura 4.53 se observa el registro de eventos que el equipo a medida se van dando se muestran en forma de línea de comando. Por otro lado en la figura 4.54 se observan las graficas producidas por los logs almacenados

en el equipo, que sin duda no son del todo claras ni útiles si se requirieren detalles específicos de eventos suscitados, ya que se enfocan en su totalidad en describir el tipo de tráfico y el tipo de servicio que se utilizó.

Log Type: Event Log

1 / 3 Column Settings Raw Clear All Filters

#	Date	Time	Level	User Interface	Action	Message
1	2008-07-21	18:03:04	information	https(172.16.64.50)	logout	Administrator admin timed out on https(172.16.64.50)
2	2008-07-21	15:54:56	warning			
3	2008-07-21	15:54:56	warning			<01350> application imd
4	2008-07-21	15:54:56	warning			<01350> firmware Fortigate-100A 3.00,build0662b662,080317 (Release)
5	2008-07-21	14:28:53	warning			
6	2008-07-21	14:28:53	warning			<00658> application imd
7	2008-07-21	14:28:53	warning			<00658> firmware Fortigate-100A 3.00,build0662b662,080317 (Release)
8	2008-07-21	10:49:09	information	https(172.16.64.50)	login	Administrator admin logged in successfully from https(172.16.64.50)
9	2008-07-21	09:38:22	notice	GUI(172.16.64.50)		User admin added antispam IP black/white entry 200.35.190.56 from GUI(172.16.64.50)
10	2008-07-21	09:38:02	notice	GUI(172.16.64.50)		User admin added antispam IP black/white entry 172.16.64.1 from GUI(172.16.64.50)
11	2008-07-21	09:33:50	notice	GUI(172.16.64.50)		User admin added URL filter entry www.juniper.com from GUI(172.16.64.50)
12	2008-07-21	09:33:35	notice	GUI(172.16.64.50)		User admin added URL filter entry www.elsalvador.com.sv from GUI(172.16.64.50)
13	2008-07-21	09:32:53	notice	GUI(172.16.64.50)		User admin added URL filter entry www.hi5.com from GUI(172.16.64.50)
14	2008-07-21	09:32:39	notice	GUI(172.16.64.50)		User admin added URL filter entry www.google.com from GUI(172.16.64.50)
15	2008-07-21	09:31:04	notice	GUI(172.16.64.50)		User admin added webfilter exempt word entry cisco* from GUI(172.16.64.50)
16	2008-07-21	09:29:22	notice	GUI(172.16.64.50)		User admin added webfilter banned word entry viagra from GUI(172.16.64.50)
17	2008-07-21	09:29:22	notice	GUI(172.16.64.50)		User admin deleted webfilter banned word entry sex from GUI(172.16.64.50)
18	2008-07-21	09:29:13	notice	GUI(172.16.64.50)		User admin added webfilter banned word entry *sex* from GUI(172.16.64.50)
19	2008-07-21	09:28:58	notice	GUI(172.16.64.50)		User admin added webfilter banned word entry sports from GUI(172.16.64.50)
20	2008-07-21	09:26:11	notice	GUI(172.16.64.50)		User admin added webfilter banned word entry chat from GUI(172.16.64.50)
21	2008-07-21	09:25:41	notice	GUI(172.16.64.50)		User admin added webfilter exempt word entry mail from GUI(172.16.64.50)
22	2008-07-21	09:25:21	notice	GUI(172.16.64.50)		User admin added webfilter exempt word entry tecno from GUI(172.16.64.50)
23	2008-07-21	08:46:57	information	https(172.16.64.50)	login	Administrator admin logged in successfully from https(172.16.64.50)
24	2008-07-21	07:47:11	information			Assigns IP address/configuration parameters to the client
25	2008-07-21	07:47:11	information			Client requests IP address/configuration parameters
26	2008-07-21	07:47:11	information			Server responds with offer of configuration parameters
27	2008-07-21	07:47:11	information			A client broadcasts a DHCPDISCOVER message
28	2008-07-21	07:47:06	information			Server responds with offer of configuration parameters
29	2008-07-21	07:47:06	information			A client broadcasts a DHCPDISCOVER message
30	2008-07-21	07:47:05	information			A client broadcasts a DHCPDISCOVER message
31	2008-07-20	01:00:16	information	https(172.16.64.53)	logout	Administrator admin timed out on https(172.16.64.53)
32	2008-07-20	01:00:16	information	https(172.16.64.50)	logout	Administrator admin timed out on https(172.16.64.50)
33	2008-07-20	01:00:16	information	https(172.16.64.50)	logout	Administrator admin timed out on https(172.16.64.50)
34	2008-07-19	22:43:35	information	jsconsole	logout	Administrator admin timed out on jsconsole

Figura 4.53 Logs almacenados en el equipo.

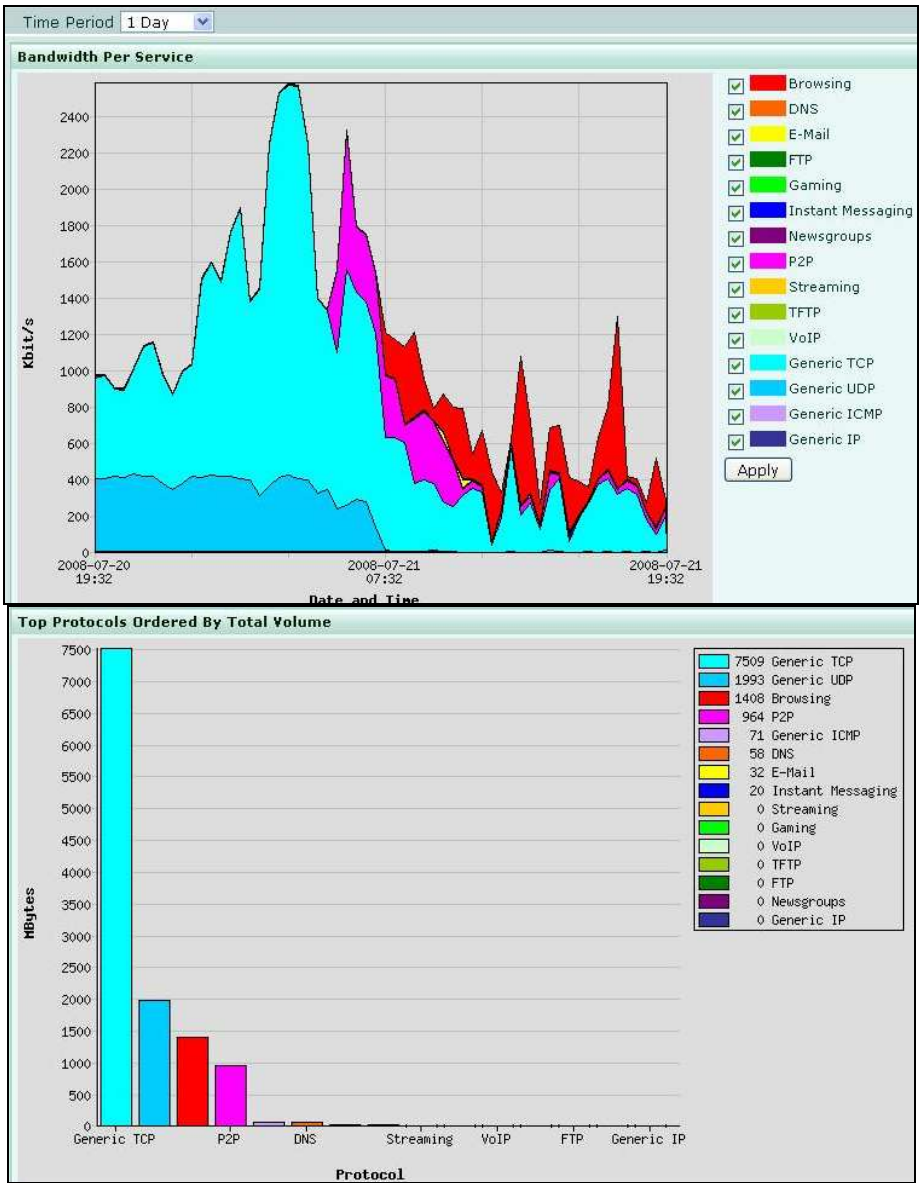
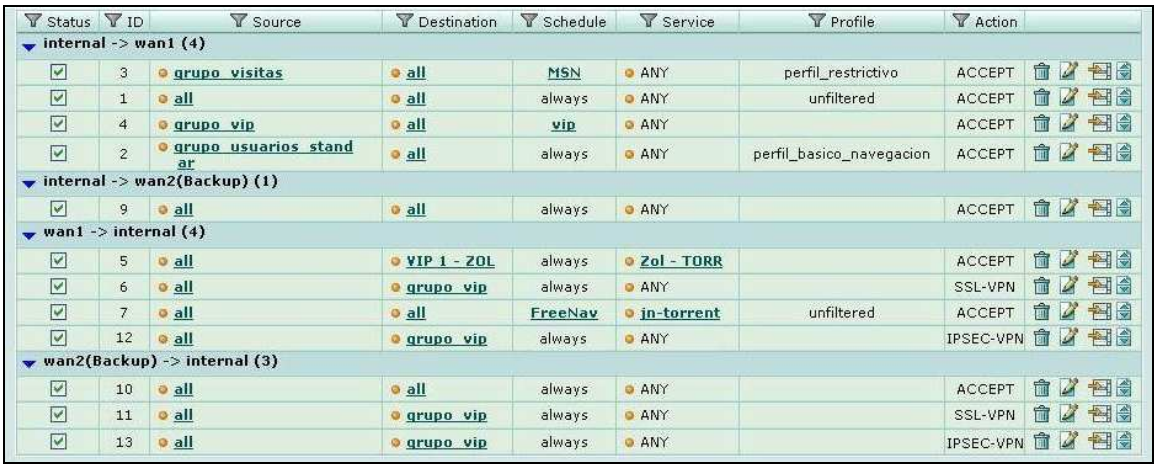


Figura 4.54 Graficas generadas a partir de los logs almacenados en el equipo.

Finalmente se presenta la imagen de las políticas configuradas en el equipo, como se puede observar, las configuraciones descritas anteriormente se presentan en la imagen 4.55.



Status	ID	Source	Destination	Schedule	Service	Profile	Action
internal -> wan1 (4)							
☑	3	grupo_visitas	all	MSN	ANY	perfil_restrictivo	ACCEPT
☑	1	all	all	always	ANY	unfiltered	ACCEPT
☑	4	grupo_vip	all	vip	ANY		ACCEPT
☑	2	grupo_usuarios_standar	all	always	ANY	perfil_basico_navegacion	ACCEPT
internal -> wan2(Backup) (1)							
☑	9	all	all	always	ANY		ACCEPT
wan1 -> internal (4)							
☑	5	all	VIP 1 - ZOL	always	Zol - TORR		ACCEPT
☑	6	all	grupo_vip	always	ANY		SSL-VPN
☑	7	all	all	FreeNav	in-torrent	unfiltered	ACCEPT
☑	12	all	grupo_vip	always	ANY		IPSEC-VPN
wan2(Backup) -> internal (3)							
☑	10	all	all	always	ANY		ACCEPT
☑	11	all	grupo_vip	always	ANY		SSL-VPN
☑	13	all	grupo_vip	always	ANY		IPSEC-VPN

Figura 4.55 Políticas finales aplicadas en el equipo

4.3 SonicWALL

Fundada en 1991 en Sunnyvale California por los hermanos Screekanth y Sudhakar Ravi, en un inicio desarrollando componentes para Apple hasta que en 1997 iniciaron con los productos de seguridad. La compañía consta con productos de seguridad UTM, dispositivos especializados en la creación de VPN, en seguridad de correo y en dispositivos especializados en backup de información para empresas. En la figura 4.56 se muestra el logo representativo de SonicWALL.

Figura 4.56 Logo de SonicWALL

4.3.1 Aspectos generales

El fabricante SonicWALL ofrece diversos equipos para igual número de aplicaciones en el ambiente informático, entre ellos podemos mencionar: UTM, VPN Secure Remote Acces, Email Security, Bakckup & Recovery, Centralised Management & Reporting entre otros. Para nuestro estudio utilizaremos el grupo de UTM, el cual a su vez se divide de acuerdo a su capacidad de manejo de usuarios en las series siguientes: TZ, PRO, NSA y E'Class NSA; todos estos a su vez se han diseñado para reducir costes, los riesgos y la complejidad

mediante la integración de funciones de seguridad dinámicas y automáticas que aseguran una protección exhaustiva y un máximo rendimiento.

Para nuestro caso se utilizo el modelo TZ 190 que está diseñado para la protección de pequeñas oficinas y sucursales remotas, este modelo tiene la característica de proporcionar conexión wireless mediante el uso de una tarjeta externa. Este equipo ofrece las siguientes características de seguridad: Firewall, Filtrado de Contenido Web, Antivirus, Antispyware, IPS, VPN, Almacenamiento de Logs, VoIP. En la figura 4.57 se presenta una ilustración de las amenazas más comunes de la red.

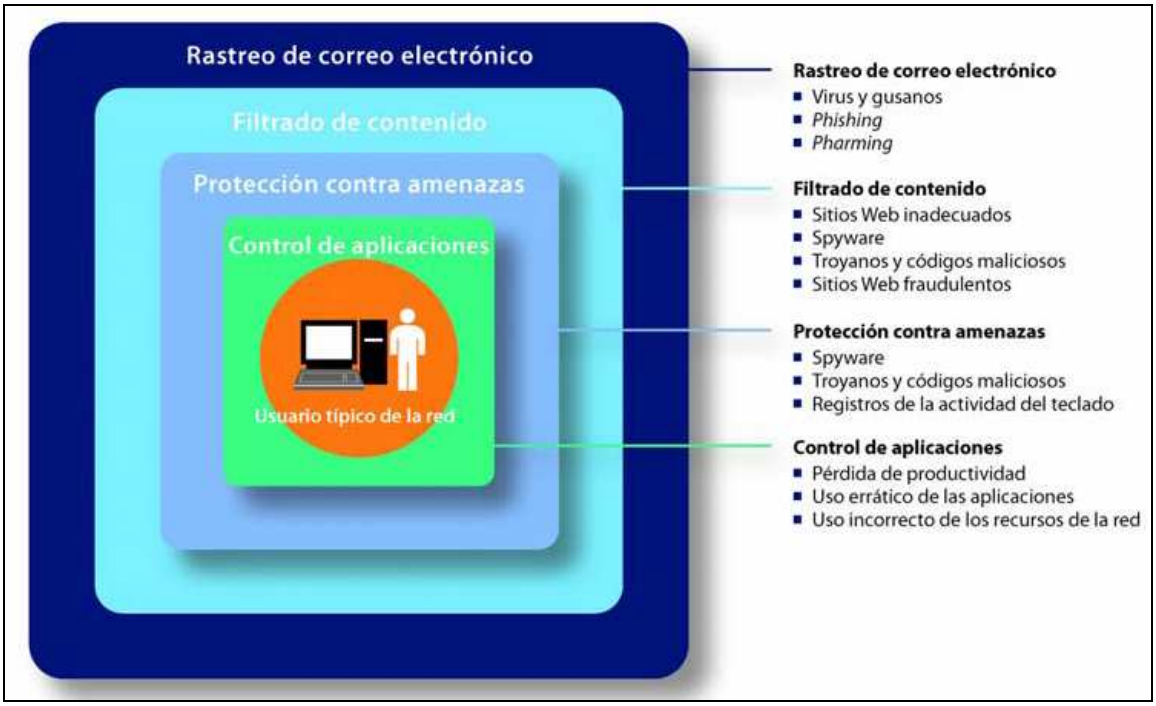


Figura 4.57 Ilustración de amenazas más comunes.

Estos equipos utilizan en su estructura interna en la parte de hardware específicamente del procesador, la tecnología Multi-Core Processor la cual según los datos proporcionados por el fabricante en su página web, proporcionan mayor velocidad y desempeño en el análisis de tráfico e identificación del mismo en tiempo real, esto al compararse con la tradicional técnica ASIC en los procesadores de otros UTM. En cuanto al software de estos equipos, es llamado SonicOS como se supone este es propietario del fabricante para garantizar una mayor seguridad en su interior.

4.3.2 Técnicas utilizadas

Como es costumbre en el caso de este tipo de equipos, se cuenta con licencias que se actualizan periódicamente para garantizar la protección dinámica del mismo, estas licencias pueden ser adquiridas en conjunto o únicamente adquirir las que el usuario requiera. La lista total de licencias incluye: Content Filter, Client AV Enforcement, Gateway Antivirus, Anti-Spyware, IPS y E-Mail Filter. El equipo de por si ofrece la ventaja de utilizar versiones de prueba en el mismo por un periodo de tiempo definido en caso de no contarse con las versiones validas del mismo y querer comprobar la funcionalidad de estas. En la figura 4.58 se observa la ilustración grafica de las licencias que el dispositivo proporciona.

Figura 4.58 Ilustración de las licencias

SonicWALL tiene segmentado el método de acción según el tipo de tráfico identificado, a continuación se presentan los análisis utilizados con sus respectivos análisis:

- *SonicWALL Gateway Anti-Virus, IPS & Anti-Spiware*: proporciona a la red protección y seguridad inteligentes en tiempo real contra una amplia gama de amenazas dinámicas, entre las que se incluyen virus, spyware, gusanos, troyanos y vulnerabilidades de software. Como capa añadida de seguridad, esta potente solución proporciona protección a nivel de aplicación contra ataques procedentes no solo del exterior sino también de la propia red interna. Este apartado cierra las puertas traseras, inspeccionando una gran numero de protocolos de correo electrónico, transferencias de archivos, flujos de datos, así como aplicaciones IM y P2P.

  Esto se realiza de la siguiente manera:

- Un motor de escaneo de paquetes gestiona tamaños limitados de archivos y virtualmente cientos de miles de descargas simultáneas.

- Utiliza una base de datos actualizada periódicamente que contiene miles de definiciones de ataques, vulnerabilidades, IM y P2P.

- *SonicWALL Content Filtering Service:* proporciona a los administradores del equipo un mayor control para reforzar transparentemente las políticas de productividad y protección, así como para bloquear contenido web inadecuado, peligroso o malicioso.

  Esto se realiza utilizando bases de datos propietarias, donde se almacenan millones de direcciones URL, direcciones IP y sitios web. Según sea el perfil configurado en el equipo se dará o no acceso al sitio consultado, esto según sea configurado el perfil en la categorización de páginas web (alrededor de cincuenta). Si la pagina web fue aceptada se almacena en cache para tener un acceso más rápido en la próxima consulta a este sitio. Permitiendo controlar el tráfico proveniente desde las interfaces LAN, interfaz wireless y VPN.

- *SonicWALL Enforced Client Anti-Virus, Anti-Spyware:* genera una protección completa antivirus y antispyware desarrollado en conjunto con McAffe, ofreciendo protección reforzada y actualizada de manera automática gracias a las definiciones de virus y de software a nivel de sistema, eliminando el lento proceso de instalación de equipo por equipo. Al combinar el cliente con la protección avanzada del servidor, se potencia las soluciones antivirus de McAffe VirusScan Enterprise para Windows y GroupShield para Exchange para servidores de archivos, de impresión y correo.

En gran medida el equipo se vale de la inspección profunda de paquetes para determinar el tipo de tráfico circulante en la red, esta es técnica es usada en tiempo real con el apartado de antivirus, antispyware, prevención de intrusiones, filtrado de contenido y la accesibilidad inalámbrica del equipo. En la figura 4.59 se muestra la ilustración de la arquitectura del análisis profundo realizado por el equipo.

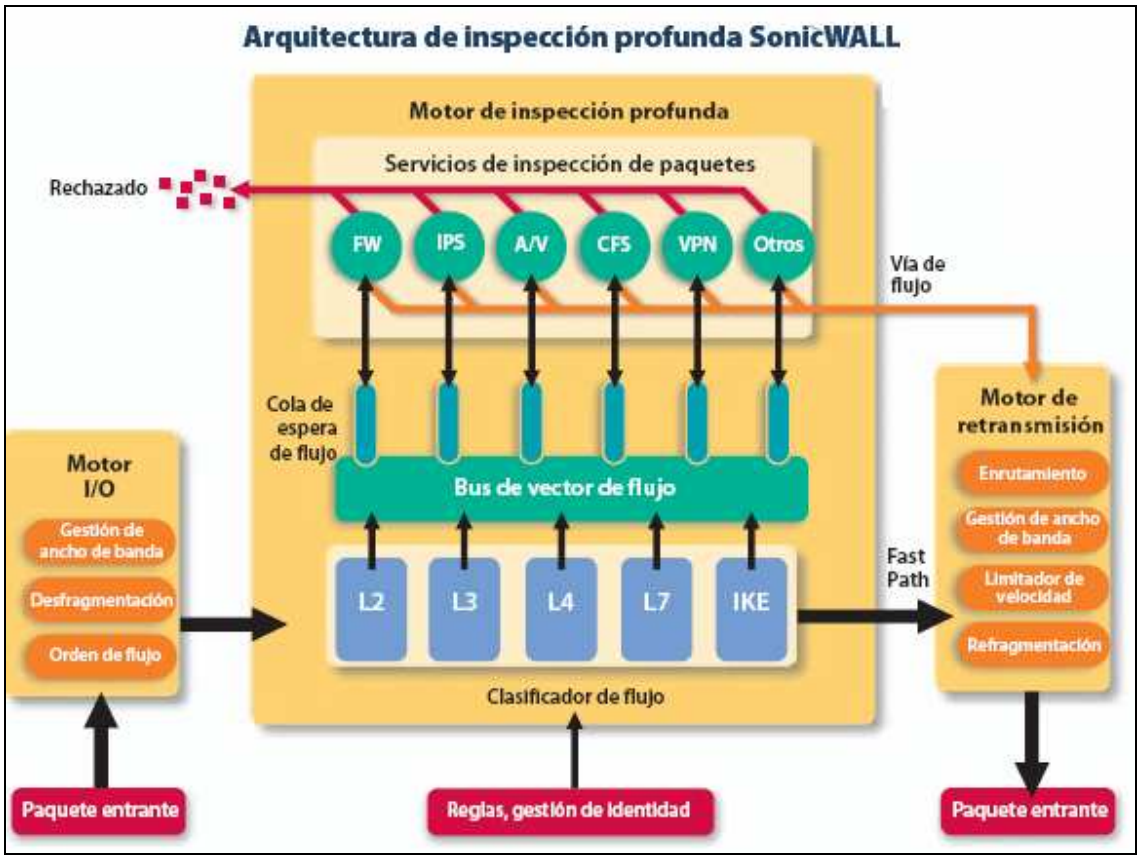


Figura 4.59 Arquitectura de Deep Packet Inspection de SonicWALL

4.3.3 Equipo SonicWALL

4.3.3.1 Elementos generales

En la ventana principal se observan estadísticas del desempeño del equipo en lo que se refiere a las aéreas de IDS, Antivirus, Spyware y aplicaciones IM/P2P, identificando todas las aplicaciones que se han detectado de cada área especifica en periodos de tiempo definidos, este equipo es capaz de almacenar estos datos desde un rango de las últimas 12 horas hasta en un rango de máximo de tiempo de los últimos 6 meses. Los datos estadísticos pueden ser generados en una especie de reporte en formato PDF con solo dar clic en la parte superior derecha de la misma ventana. Lo anterior se presenta en la figura 4.60.

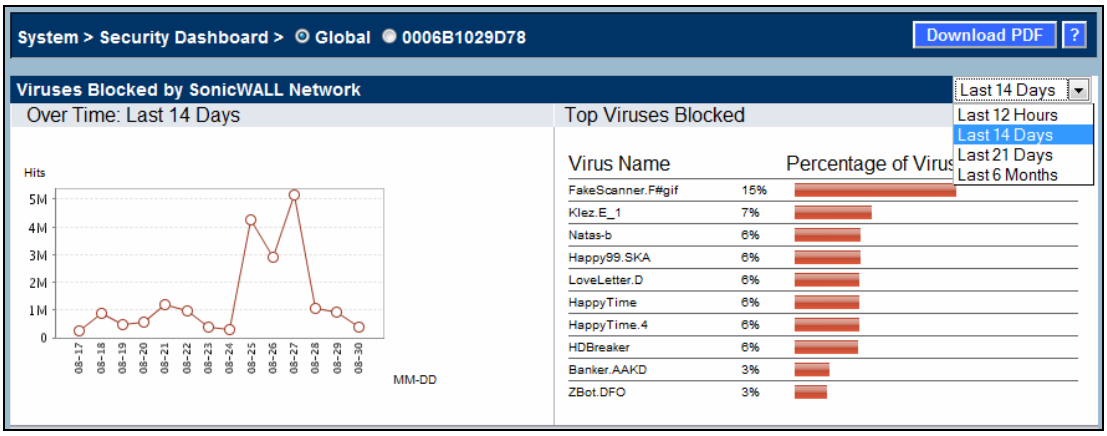


Figura 4.60 Pagina principal de equipo SonicWALL

En la segunda ventana presentada se observan datos del equipo como la información del equipo como el modelo y datos técnicos del mismo; de la misma manera se observan los servicios habilitados para la protección del mismo; así como las ultimas alarmas registradas por el dispositivo; se presentan además las interfaces con las que el equipo cuenta mostrando las IP y el estatus de las mismas; finalmente se presenta en la parte superior derecha de la ventana los Wizards o elementos auxiliares para las configuraciones básicas del equipo; los puntos mencionados se presentan en la figura 4.61.

Figura 4.61 Ilustración de la ventana de datos generales.

El acceso a las diferentes secciones del equipo se presentan en forma de menú vertical en el lado izquierdo de la pantalla, los cuales a su vez se subdividen en apartados más específicos, de ser necesario estas hacen referencia a configuraciones que dependiendo de la naturaleza del apartado pudiese estar ligada a otros elementos del menú. En la figura 4.62 se presenta el menú principal del equipo.

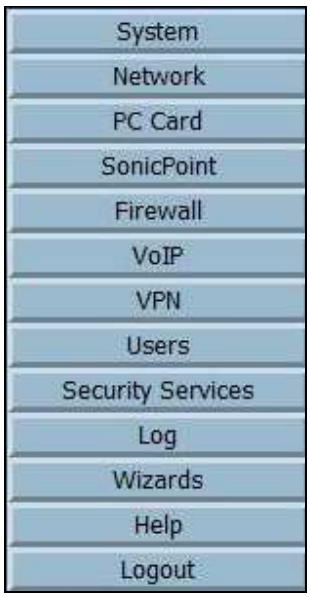


Figura 4.62 Menú principal

4.3.3.2 Descripción del menú principal y las sub categorías más importantes

a) System.

Security Dashboard: presenta los datos estadísticos del desempeño del equipo en cuatro aéreas específicas IDS, Antivirus, Spyware y aplicaciones IM/P2P. Estas pueden ser fácilmente proporcionadas en forma de reporte en formato PDF.

Status: se muestran datos generales del equipo como su versión, la capacidad de memoria interna, el procesador, ultimas alarmas, estatus de las licencias y de las interfaces físicas.

Licenses: como su nombre lo indica, presenta los servicios de seguridad como Antivirus, AntiSpam, cliente de VPN, autenticación de usuarios, etc. con los que el equipo cuenta, así como el tipo de licencia y la fecha de caducidad de las mismas,

además desde este apartado se pueden actualizar o renovarlos servicios manualmente.

Administration: permite configurar parámetros de acceso al equipo como el usuario, el password del mismo, el tiempo de logeo antes de finalizar la sesión por inactividad, los puertos utilizados para protocolos como HTTP, HTTPS, SSH y SNMP.

Certificates: muestra los certificados digitales con los que el equipo cuenta entre ellos se pueden mencionar los CA (Certificate Authority) de SSL, certificados de Microsoft y del mismo SonicWALL, mostrando además el tipo de certificado registrado y la fecha de caducidad de las mismas.

Time: permite la sincronización del equipo con servidores de NTP alrededor del mundo, entre los cuales se elige la hora del sistema que el usuario prefiera, de la misma manera es posible sincronizarlo con algún otro equipo de NTP si es que el usuario lo considera necesario.

Schedules: desde este apartado se crean horarios recursivos para luego asociarlos a usuarios o perfiles específicos. Por defecto el equipo ya trae definidos tres horarios por defecto los cuales son para horas de trabajo, fines de semana y horas de no trabajo en la semana. Se pueden agregar según se deseen siempre y cuando se tome en cuenta que estos serán recursivos en las semanas posteriores.

Settings: hace referencia a la versión de SonicOS con las que cuenta el equipo, tanto a la versión actual como con la versión con la que originalmente conto el equipo desde su fabricación, así como las versiones de backup’s con que el equipo puede disponer.

Packet Capture: como su nombre lo indica, hace referencia a la captura de paquetes que el equipo ha realizado, el detalle del paquete capturado, las IP involucradas en el trafico, el tipo de trafico utilizado, la interfaz utilizada, así como a la acción que se tomo luego de identificar el mismo.

Diagnostics: permite el acceso a un reporte detallado del trafico que ha circulado por el equipo, detallando las IP’s, los protocolos usados, los puertos, las claves cifradas, etc. Este reporte puede ser enviado por medio de un correo electrónico o por medio del botón ubicado en esta sección. Por otro lado permite además, monitoreo de herramientas de diagnostico como ping, traceroute, nslookup entre otras hacia IP definidas y también permite observar elementos estadísticos del equipo como la utilización del CPU, la verificación de IP’s en listas negras o la captura de paquetes.

Restart: reinicia el equipo.

b) Network

Interfaces: desde aquí es posible la visualización de las interfaces físicas del equipo, observando las configuraciones de IP en cada una, el estatus físico y las estadísticas de tráfico que han circulado por ellas.

Switch Ports: en este apartado es posible la visualización de los puertos destinados a la LAN, aquí se puede observar la configuración y conexión física de cada uno, además de poder modificar la configuración lógica del conjunto mencionado, ya que pueden configurarse como 8 puertos de un mismo segmento o como cuatro puertos de dos segmentos separados o viceversa.

WAN Failover & LB: permite configurar el balanceo de carga entre las interfaces WAN en caso de contar con dos ISP diferentes o utilizar un enlace como principal y el otro como secundario. Así mismo permiten la configuración del monitoreo de las interfaces cada cierto tiempo.

Zones: como su nombre lo indica, en esta sección se visualizan las aéreas que se han creado en el equipo, así como el tipo de seguridad aplicado a cada una y las licencias que analizan el trafico circulante por cada una.

DNS: permite la configuración de tres DNS directamente en el equipo.

Address Objects: presenta las direcciones creadas en el dispositivo luego de configurar las interfaces del mismo, además permite agregar IP’s a objetos específicos en diferentes zonas de trabajo, luego estos objetos pueden ser agrupados por nombres definidos para luego poder asociarse a políticas o accesos definidos en los posteriores apartados.

Routing; aquí se visualizan las rutas auto-creadas luego de la configuración de las interfaces del equipo, estas son las necesarias para que el equipo tenga acceso a Internet; además se pueden agregar rutas especificas utilizando las interfaces existente así como los objetos creados en el punto anterior.

NAT Polices: al igual que el punto anterior en este apartado se visualizan las políticas de NAT creadas por el mismo equipo luego de la configuración de las interfaces WAN y LAN. De la misma manera permite la configuración de políticas de NAT que el usuario considere necesarias, especificando las interfaces por las que circulara y la traducción de IP a realizarse.

ARP: desde este apartado es posible la asociación de IP fijas con MAC Address de equipos definidos, estas se asocian a interfaces del equipo para evitar que una MAC Address puede tener acceso desde otro punto diferente al configurado. De la misma manera en esta sección es posible observar las MAC Address registradas por el equipo con las respectivas IP utilizadas.

DHCP Server: permite la creación de servidor DHCP desde el equipo, haciendo posible definir el rango del que se otorgaran las IP's, además de definir la interfaz que se utilizara para este fin.

IP Helper: permite la configuración de un IP Helper con el equipo, estableciendo las interfaces que se verían involucradas.

Web Proxy: da la opción a realizar la interconexión de un servidor Proxy con el dispositivo, únicamente se requiere la IP del Proxy y el puerto por el cual se comunicara.

Dynamic DNS: permite la interconexión con servidores dinámicos de DNS en Internet para realizar la resolución de nombres, definiendo el usuario y el password en cada sitio a solicitar dicho proceso.

c) PC Card

Status: indica si existe alguna tarjeta para conectividad inalámbrica colocada en el dispositivo.

Settings: desde este apartado es posible la configuración de tarjetas ya sea wireless o cable modem en el equipo, con el fin de agregar funciones extras en el mismo.

SonicPoint: permite la configuración de comunicación del equipo con diferentes tecnologías en Access point, esto con el fin de proporcionar un mayor alcance al segmento wireless en caso de ser necesario.

Station Status: indica la conectividad del equipo con repetidores inalámbricos.

IDS: el primer apartado de este segmento permite agregar mecanismos de seguridad en la accesibilidad wireless, indicando el segmento de red que puede tener acceso a la parte inalámbrica del mismo, de la misma manera permite limitar el acceso a MAC Address definidas en el equipo. El segundo apartado nos muestras los Access points que pudiesen estar disponibles para conectarse con el dispositivo.

d) Firewall

Access Rules: controlar el acceso o la comunicación entre interfaces es posible realizarlo desde aquí, indicando las interfaces en cuestión, el destino del tráfico, el tipo de servicio, los usuarios. De la misma manera muestra una pequeña estadística del tráfico que ha circulado utilizando cada regla de acceso configurada. Sin la correcta configuración y asociación de parámetros en este apartado sería inútil la creación de políticas en los segmentos externos.

Advanced: este apartado ofrece varias alternativas de configuraciones avanzadas en el equipo. Entre las características más importantes se pueden mencionar que permite la configuración de protección ante ataques de hackers, denegación de paquetes ICMP, habilitación de puertos específicos para aplicaciones que requieran bases de datos como Oracle, soporte para Windows MSN, control de acceso a aplicaciones FTP, el manejo de puertos alternativos a aplicaciones especificas y la limitación de ancho de banda por conexiones establecidas.

TCP Settings: muestra las estadísticas del tráfico TCP detectado, denegado y circulante en el equipo. Además permite habilitar Stateful Inspection en los paquetes TCP, asi como la protección a ataques de SYN Floods utilizando diversos métodos desde las interfaces del equipo, finalmente permite la creación de listas negras en base a las MAC Address detectadas como generadoras de ataques.

Services: permite la visualización de los servicios identificados por el equipo, de la misma manera permite la asociación de estos en grupos específicos con el fin de tener un mejor control de estos, por otro lado se pueden crear servicios específicos para aplicaciones necesarias configurando el tipo de protocolo a utilizar y el rango de puertos usados por la misma.

Multicast: permite la configuración contra ataques de esta naturaleza como el snooping, generando políticas definidas de escuchas con direcciones que generan multicast desde cualquier interfaz del equipo incluyendo las VPN que se utilizan.

Conections Monitor: desde este apartado es posible la visualización de las conexiones establecidas en el equipo, identificando las IP’s y puertos origen y destino, los protocolos usados y las interfaces usadas para esto. Además permite el filtrado de datos para luego generar reporte de las conexiones establecidas por alguna IP específica o algún tipo de tráfico determinado.

VoIP: en esta sección se tiene acceso a la manipulación de tráfico de VoIP, permitiendo establecer la configuración para entablar llamadas por cualquiera de las

interfaces del equipo, utilizando los protocolos H.323 y SIP. Para este tipo de tráfico muchas veces se requiere la configuración de QoS o de políticas específicas, si bien es cierto, estas no se realizan desde este apartado pero si es posible complementar la configuración de este apartado con las secciones antes descritas.

Call Status: muestra el registro de las llamadas de VoIP que se han efectuado.

e) VPN

Settings: desde aquí es posible realizar la configuración de las políticas de una VPN, definiendo el tipo de cifrado a utilizar, además de los datos necesarios para establecer una comunicación segura como el protocolo de autenticación IKE y los parámetros necesarios para configurar una VPN IPSec. En este mismo apartado se pueden observar los túneles VPN activo. Este apartado también cuenta con un wizard para ayudar a la creación de la misma.

Advanced: permite el establecimiento de parámetros adicionales en la creación de VPN, entre ellos se pueden mencionar la detección de fragmentos maliciosos a la hora de establecer las sesiones de autenticación IKE, de recibir los parámetros de cifrado necesarios para establecer una VPN o establecer la verificación OCSP (Online Certificate Status Protocol) del canal establecido.

DHCP over VPN: como su nombre lo indica, el equipo es capaz de entregar o recibir servicio DHCP hacia o desde las conexiones remotas según se requiera.

L2TP Server: permite la configuración de ser un servidor VPN L2TP sobre IPSEC mientras que en el otro extremo se requerirá de un cliente que se desenvuelva de la misma manera. En donde se puede determinar los usuarios internos que tendrán acceso a esta conexión remota.

f) Users

Status: esta sección permite visualizar los usuarios que están activos en el equipo, indicando la IP desde cual se accesa y el tiempo restante en dicha conexión.

Settings: desde este apartado es posible definir el método de autenticación que el equipo utilizara para sus usuarios, este puede ser el mismo equipo o interconectarse con bases de datos externas. De la misma manera es posible establecer el tiempo de

sesión para los usuarios locales y definir las interfaces desde las cuales se permitirá el acceso a dichos usuarios.

Local Users: se presenta la visualización de los usuarios locales existentes junto con los accesos otorgados a cada uno. Además desde esta ubicación es posible agregar usuarios al equipo y asignarles grupos definidos.

Local Groups: permite crear grupos con los usuarios que el equipo tiene registrados, a estos se les puede asignar perfiles web que luego son asociados a políticas de acceso.

Guest Services: permite configurar accesos temporales a usuarios que requieran el acceso a la red interna en un periodo de tiempo. Estos usuarios pueden ser agregados de la misma forma a los usuarios locales antes descritos.

Guest Accounts: los usuarios temporales que se configuraron en el punto anterior, pueden ser asociados a una cuenta especifica desde donde se pueden autogenerar contraseñas automáticas estas cuentas desde el momento que se asocian empiezan con una especie de conteo regresivo en donde cumplen el tiempo para el cual fue creada dicha cuenta, esto para evitar que cualquier persona se autentique con algún perfil temporal o que ese perfil quede accesible luego del tiempo estipulado.

Guest Status: desde este apartado se puede observar los usuarios temporales que están registrados en el equipo al momento de consultar este apartado.

g) Security Services

Summary: permite ver en resumen el estado de las licencias y realizar una sincronización manual de estas. De la misma manera se puede escoger el nivel de seguridad deseado, finalmente se presenta una breve descripción de los sistemas de seguridad con lo que el equipo cuenta.

Content Filter: desde este apartado es posible la configuración del filtrado de contenido web, este se puede realizar desde las licencias activas del equipo o desde agentes externos al mismo como Websense o N2H2. De la misma manera se puede restringir el acceso a ventanas emergentes o a dominios específicos. Por otro lado también es posible agregar sitios que se puedan excluir del control de contenido dinámico que se genera con las licencias. Finalmente es posible editar con formato HTML los mensajes que aparecerán en caso de presentarse el bloqueo de algún sitio web.

Client AV Enforcement: muestra el número de licencias de clientes anti virus activas además de la fecha de expiración de las mismas, es decir de usuarios finales. En la segunda parte se puede observar la administración de las licencias AV, con la opción de crear un reporte de las capturas realizadas. Finalmente da la opción de configurar cada cuanto se realizara la búsqueda de actualizaciones, así como forzar la actualización luego de detectar niveles de riesgo, por ultimo ofrece la opción de forzar la aplicación de estas licencias a todos los usuarios posibles o de excluir el trafico circulante entre dos IP fijas.

Gateway Antivirus: este es la protección perimetral que ofrece el equipo propiamente dicho. Se presenta en primer lugar la versión de firmas que se está utilizando, la fecha que esta expira, así como los protocolos que están sometidos a análisis http, FTP, IMAP, POP3. SMTP y TCP Stream. Finalmente se visualizan todas las firmas con las que el equipo cuenta para generar el análisis de archivos de manera eficiente.

Prevention: muestra las firmas con las que cuenta el equipo así como la fecha de caducidad de las mismas. Luego se permite la configuración de las firmas, estas pueden ser únicamente para identificar las amenazas o para prevenir las mismas, también se puede configurar para que una vez identificada una amenaza esta no sea detenida sino que se deje el paso libre para ella.

Anti-Spyawre: presenta en la primera parte las firmas utilizadas así como la fecha de expiración de las mismas. Luego se puede observar los tres niveles de grupos de firmas que pueden ser configuradas para detectar las amenazas y para proteger de las mismas; posteriormente se presentan los protocolos para los cuales se activan las firmas http, FTP, IMAP, SMTP y POP3; de igual manera es posible configurar el mensaje a presentar cuando se bloquea el acceso de algún archivo y también es posible excluir archivos el análisis entre IP's fijas. Finalmente se presenta el listado de las firmas utilizadas para la protección de archivos.

E-Mail Filter: muestra la configuración de las protección de correo, la cual se puede configurar para el análisis de los archivos adjuntos o para extensiones especificas las cuales pueden ser definidas por el administrador del equipo. También se permite configurar el mensaje a mostrar por el equipo una vez detecta algún archivo sospechoso, de la misma manera presenta la opción de bloqueo de fragmentos de paquetes SMTP.

RBL Filter: permite la activación de la protección RBL así como la resolución de los DNS para estas aplicaciones, por otro lado define por defecto dos servidores de protección contra RBL que contienen en su interior Black List, sin embargo permite

agregar las que el administrador considere necesario. De la misma manera es posible configurar SMTP servers ubicados en interfaces definidas del equipo.

h) Log

View: como su ubicación supondría, presenta los logs que el equipo ha podido capturar de los eventos que se han suscitado, identificando la fecha, la categoría, la interfaz de origen, interfaz de destino y el tipo de protocolo utilizado para este log.

Categories: desde aquí es posible la visualización de categorías de los logs almacenados en el equipo, pudiendo configurar el nivel de los logs que el equipo almacenara y definiendo el nivel de alerta que se almacenara en el mismo.

Syslog: esta sección permite la interconexión del equipo con una base de datos syslogs para almacenar los registros de los eventos generados.

Automation: desde este apartado se puede configurar el envío de los logs por correo electrónico, este envío se puede programar para que sea cada cierto tiempo o cuando se sature la capacidad del dispositivo para almacenarlos, así no se tendrá perdida de los sucesos que el equipo ha detectado.

Name Resolution: se puede configurar para que la resolución de nombres de los logs sea por DNS o NetBios.

Reports: permite tener un mini reporte de los sitios web visitados en orden al número de visitas realizas, al ancho de banda utilizado por IP de la LAN o en base al servicio que se ha utilizado para mayores tasas de transferencia.

i) Wizards

Setup Wizard: es utilizado para lograr una configuración rápida de acceso a Internet, permite la configuración de interfaces con sus respectivas IP, el modo de operación y las zonas a utilizar.

Registration & License Wizard: recomendado para activar las licencias del equipo.

PortShield Interface Wizard: utilizado para la configuración y manejo del switch LAN del equipo, permite separar el switch de ocho puertos en grupos de cuatro o dos puertos según sea necesario.

Public Server Wizard: con este apartado se obtiene una rápida configuración para proveer acceso externo a un servidor que se encuentra en la red que se esta protegiendo.

VPN Wizard: utilizado para crear políticas de VPN ya de punto a punto o con un cliente en el sitio remoto; permite establecer los parámetros requeridos como la autenticación y la negociación necesarias para establecer el canal de comunicación.

j) Help

Permite tener acceso a la ayuda con que cuenta el equipo.

4.3.3.3 Parámetros Básicos

Las pruebas realizadas consistieron en la comprobación de aspectos básicos del equipo ya que por el poco tiempo que este dispositivo fue concedido (alrededor de siete días), solamente se pudieron realizar pruebas de nivel básico, estas se realizaron con la ayuda de los manuales que el mismo fabricante proporciona para cada apartado específico.

La configuración general: configuración de rutas estáticas, configuración de redundancia de ISP, registro y activación de licencias, verificación de parámetros de página principal.

El equipo en un inicio se entrego sin configuración alguna más que las configuraciones que por defecto el equipo posee, como los perfiles de protección antivirus, antispam, IPS y el filtrado de contenido web básico.

La configuración básica del equipo fue configurada con los Wizards con los que cuenta el equipo, primero configurando el nombre y la contraseña del usuario, luego seleccionando la zona horaria a la cual se pertenece, posteriormente definiendo las IP de las interfaces físicas, los DNS e indicando que no se utilizara una tarjeta para el acceso inalámbrico ya que este equipo permite colocarle una tarjeta externa para lograr contar con ese recurso. La configuración de las interfaces del equipo se presenta en la figura 4.63.

Name	Zone	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
LAN	LAN	172.16.64.223	255.255.255.0	Static	Connected	Default LAN	
WAN	WAN	168.243.26.251	255.255.255.248	Static	No link	Default WAN	
OPT	Unassigned	0.0.0.0	0.0.0.0	N/A	Connected		
WWAN	WAN	0.0.0.0	255.255.255.0	Dial-Up	No Device	WWAN	

Add PortShield Interface...

Figura 4.63 Configuración de interfaces en el equipo.

Después de esto, se inicio con la configuración de los perfiles para los usuarios de la red interna, que para el caso eran aproximadamente veinte, tomado en cuenta que se tendrán IP fijas por cada uno y se tiene la necesidad de generar IP disponibles para visitas esporádicas en el lugar. Se realizo la configuración de tres perfiles definidos, agrupando las IP en áreas específicas, además de crear rutas estáticas para aplicaciones que se manejan desde otras redes externas. La ilustración de esto se presenta en la figura 5.64

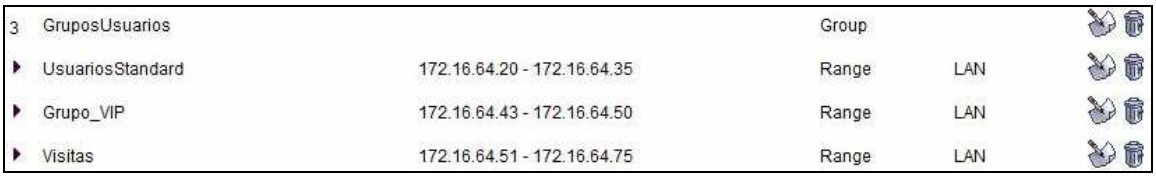


Figura 4.64 Ilustración de usuarios configurados.

Posteriormente se procedió a la configuración de un servidor DHCP en la interface LAN para rangos de IP no contemplados en los apartados anteriores, siendo posible establecer en base a MAC Address de las PC's las IP que el servidor otorgara. De igual manera se configuraron servicios como la comunidad SNMP con el fin graficar el desempeño de la red en tiempo real por un sistema de gestión presente en el sitio de prueba. Las graficas de la configuración DHCP se presentan en la figura 4.65.

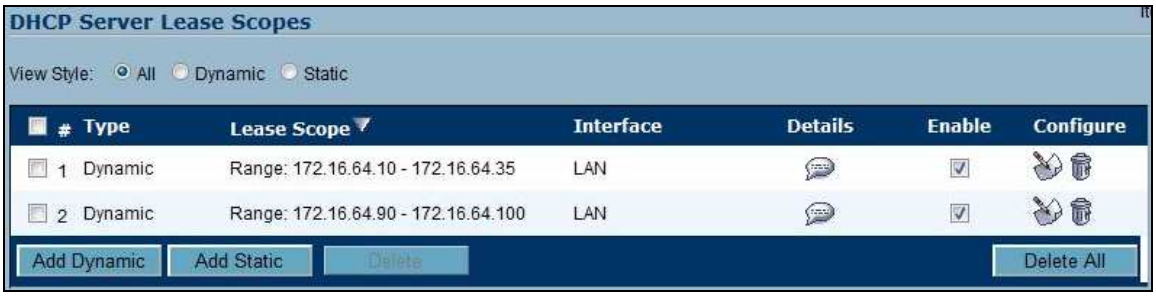


Figura 4.65 Ilustración de DHCP configurado.

4.3.3.4 Configuración de VPN

VPN IPSEC

En la parte de creación de VPN se realizo únicamente la configuración de la modalidad IPSEC, ya que el equipo no contaba con la capacidad de crear una VPN SSL, esto en parte debido a que el mismo fabricante distribuye otro dispositivo especializado para estas aplicaciones VPN que maneja diversas de estas modalidades, sin embargo otros UTM más

robustos de este mismo fabricante con las últimas versiones de SoniOS ya permiten la creación de este tipo de VPN pero únicamente establecen la comunicación entre dos dispositivos similares.

El equipo permite la configuración de IPSEC utilizando la modalidad de punto a punto donde se necesitan equipos especializados en ambas localidades, además ofrece la posibilidad de creación de Gateway remoto en donde se requiere el equipo UTM en un extremo y en el otro se utilizara un cliente en versión software que el mismo fabricante provee, el nombre de este aplicativo de cliente IPSEC es GVC.

La configuración del dispositivo se realiza en una sola fase pero en notables segmentos diferentes los cuales son necesarios de configurar para establecer la comunicación utilizando IPSEC, esto se realiza desde la ubicación *VPN / Settings* se selecciona *Add* en la sección de *VPN Polices*. Luego de configuradas los parámetros necesarios para la creación de la VPN se necesita configurar el trafico por esta interfaz lógica y asociarla a una interfaz física, esto último es lo que se necesita configurar en el equipo en cuestión, adicionalmente se pueden crear usuarios específicos para esta aplicación y horarios específicos para la utilización de la misma. En la figura 4.66 se presenta la ilustración de las fases de creación de la VPN en el dispositivo.

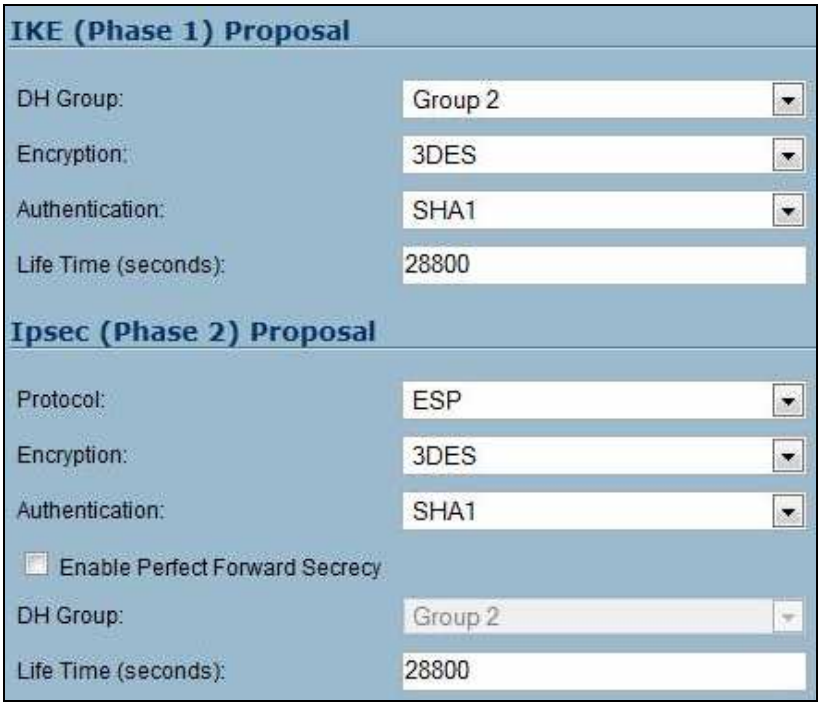


Figura 4.66 Ilustración de configuración de VPN IPSec.

Luego de la creación de los parámetros mencionados, se procede a la instalación y configuración del cliente de VPN a utilizar, primero se configura la IP pública del

dispositivo a utilizar y el nombre de la conexión, luego una vez identificado el dispositivo con la IP publica se establece la comunicación, debido a que los parámetros necesarios para la establecer la VPN en el UTM no fueron cambiados no se requerirá un mayor cambio en el cliente VPN. En la figura 4.67 se presenta la ilustración del cliente usado.

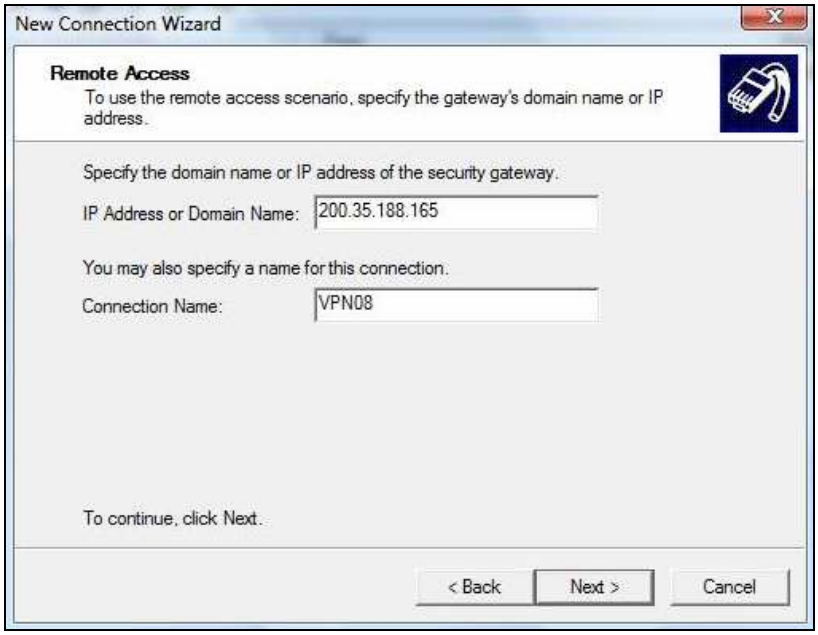


Figura 4.67 Cliente VPN utilizado en IPSec.

Una vez establecidos los parámetros en ambos dispositivos, se accede al cliente por software y se establece la conexión, luego se accesa utilizando el usuario configurado en el equipo para este fin, una vez completado el proceso se revisa que ambos dispositivos tengan establecida la sesión. En la figura 4.68 y 4.69 se muestra el establecimiento de las sesiones observado desde ambos sitios involucrados.

Figura 4.68 Establecimiento de VPN desde el servidor.

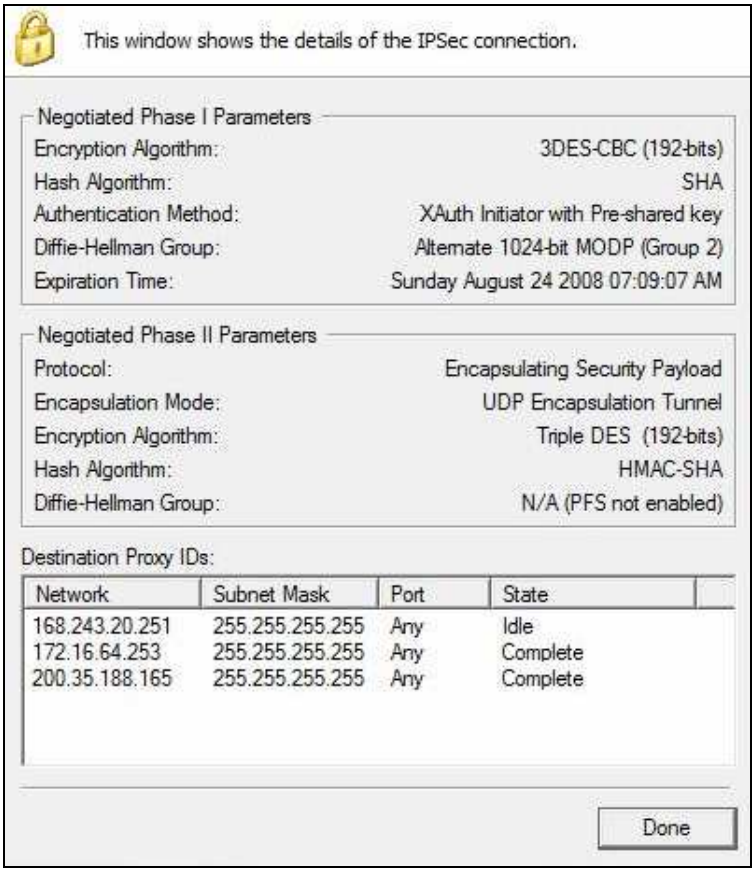


Figura 4.69 Establecimiento de VPN desde el cliente.

4.3.3.5 Configuración de perfiles.

La configuración de perfiles se puede conformar de varias maneras, la primera en comprobar es la de agrupar segmentos de IP de acuerdo a las necesidades laborales, esto se realiza desde el apartado *Network / Address Objects*, en donde primero es necesario desde la sección *Adrress Objects* crear los objetos que se van a utilizar, luego se agrupan estos objetos en la sección de *Address Groups* para luego asociarlos a políticas definidas. En este caso se crearon tres grupos de direcciones, uno para la gestión de equipos de la LAN, otro para la creación de rutas estáticas con otro segmento de la misma LAN de la empresa y otro para los usuarios presentes en la LAN; a esto hay que agregar que existen perfiles creados por defecto en el equipo los cuales son alrededor de trece. En la figura 4.70 se presenta la ilustración de los objetos y grupos de direcciones creados para las pruebas.

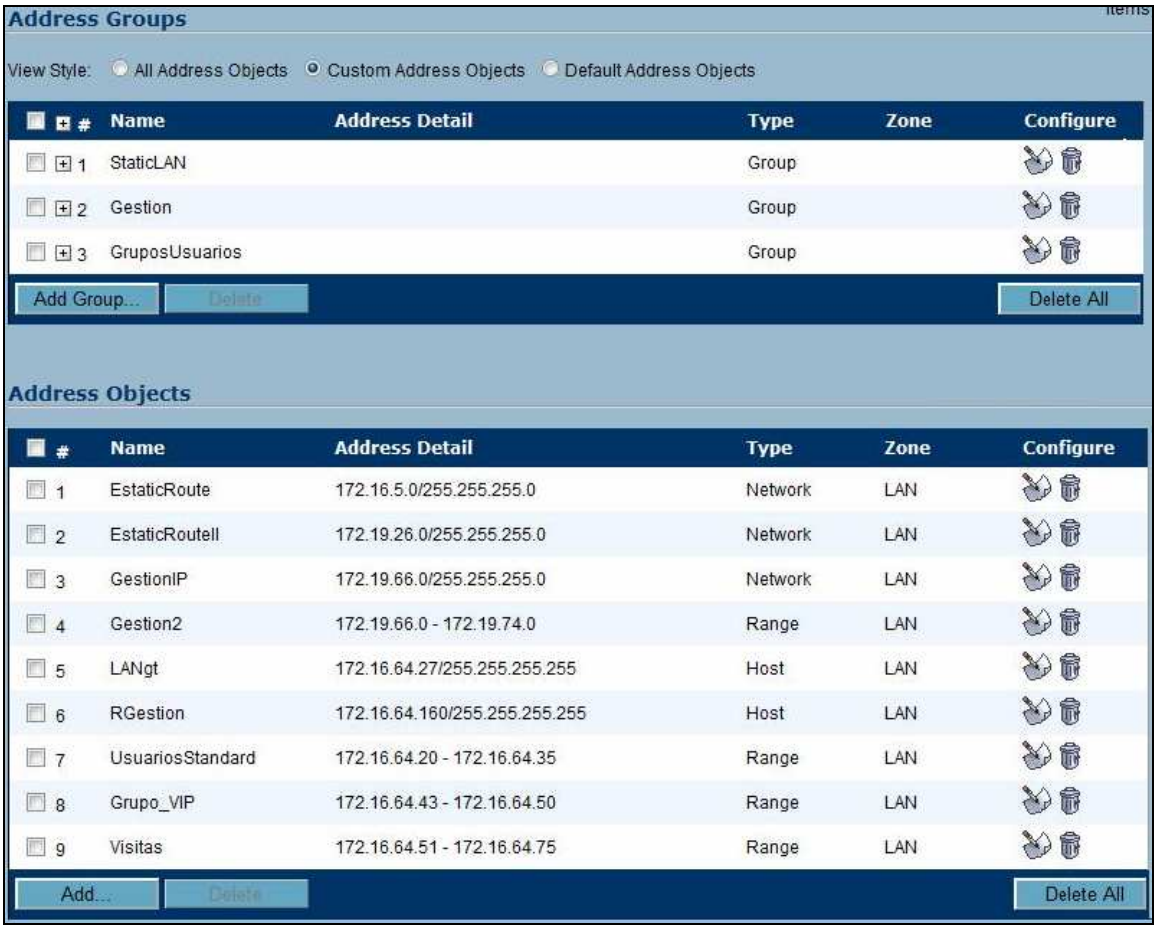


Figura 4.70 Ilustración de perfiles configurados.

Por otro lado, los usuarios pueden autenticarse directamente desde el equipo, luego estos perfiles son asociados a políticas definidas para poder controlar el acceso web o a aplicaciones requeridas. La configuración de usuarios que requieran autenticación se generara siempre y cuando no se tenga una política de acceso definida par la IP que está intentando acceder a Internet. Esta configuración se lleva a cabo desde la ubicación *Users / Local Users*, teniendo la ventaja que si se genera para un usuario especifico un perfil definido, este al logearse desde algún otro equipo tendrá siempre el mismo perfil asociado. La ilustración del logeo local se presenta en la figura 4.71.

Figura 4.71 Autenticación local de usuarios.

La autenticación de usuarios también es posible realizarlas desde dispositivos externos al equipo, como LDAP o RADIUS sin embargo para que esta configuración sea fructífera se requiere de un agente externo llamado SSO (Single Sign-On) el cual hace posible la intercomunicación entre el UTM y la base de datos externos. Estas configuraciones se realizan desde la ubicación *Users / Settings* además de las configuraciones externas que no fueron consideradas en este trabajo.

Sin embargo otro tipo de autenticación muy útil para empresas o asociaciones que reciben visitas o auditorias por periodos de tiempo considerables y que por lo tanto requieren acceso a la red local o a Internet de manera temporal, este equipo ofrece la creación de estos usuarios con un tiempo de vida regulado por el administrador, para que una vez dados de alta se inicie una especie de cuenta regresiva antes de ser dado de baja; esta configuración permite la creación de contraseñas y nombres de usuarios de manera aleatoria, garantizando así un mejor control sobre los usuarios temporales que se agregan a la red interna.

Lo antes descrito es posible configurarlo desde la ubicación *Users / Guest Services* en donde se determina el tiempo de vida del perfil creado esto se muestra en la figura 4.72, posteriormente para dar de alta se accede a la ubicación *Users / Guest Accounts,* en donde se observa la cuenta regresiva del perfil temporal asociado. Lo antes descrito se presenta en la figura 4.73

Figura 4.72 Usuarios temporales configurados

Figura 4.73 Cuenta regresiva de los usuarios temporales.

Los perfiles además se pueden controlar en base a horarios establecidos, estos horarios es posible configurarlos de manera repetitiva cualquiera de los días de la semana o incluso los

siete días de ser necesario, por defecto el equipo ya trae configurados tres perfiles, pero el usuario puede agregar los que considere convenientes para luego aplicarlos a grupos de IP o a usuarios específicos. Estos horarios es posible su configuración desde la ubicación *System / Schedules*, esto se presenta en la figura 4.74

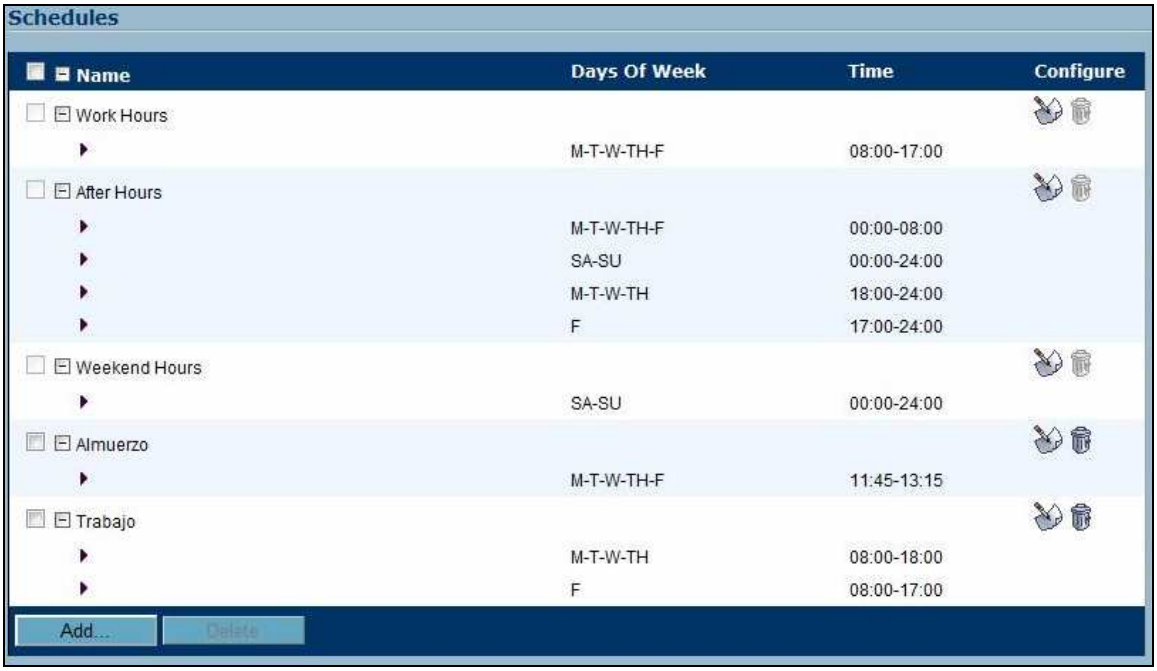


Figura 4.74 Horarios definidos

4.3.3.6 Filtrado de contenido web

El filtrado de contenido web es posible realizarlo utilizando la categorización dinámica que proveen las licencias del equipo. Estas agrupan las páginas web en base a su contenido, con la intención que el administrador del equipo seleccione las categorías con facilidad, de la misma manera se pueden excluir páginas web de estas categorizaciones con la salvedad que deben agregarse manualmente en cada perfil requerido. Lo antes descrito es posible acceder desde la ubicación *Security Service / Content Filter* seleccionando en el apartado *Content Filter Type* el botón de *Configuration*. En la figura 4.75 se presentan algunas de las cincuenta categorizaciones entre las que se puede elegir para controlar el acceso web.

Figura 4.75 Categorización web

En la pantalla principal, se puede bloquear la activación de Activex, Java, Cookies y acceso hacia http Proxy Servers. En la parte inferior de la misma pantalla se presenta la opción de configurar el mensaje de bloqueo de página si en dado caso este se llegara a necesitar para cualquier usuario. El mensaje configurado que aparecerá si alguna web es bloqueada se presenta en la figura 4.76, este mensaje es posible modificarlo a gustos de los administradores ya que es creado en lenguaje HTML.

Figura 4.76 Mensaje de restricción web.

De la misma manera es posible bloquear palabras o frases que el usuario puede configurar según considere, lo mismo sucede con dominios específicos los cuales se pueden denegar o permitir con solo agregar sus nombres a las listas indicadas, finalmente es posible la configuración de IP's definidas para denegar los accesos a las mismas. Lo anterior es posible realizarlo desde la ubicación *Security Services / Content Filter* accesando a *Configure* en la pestaña de *Custom List*, dicha ilustración se presenta en la figura 4.77.

Figura 4.77 Filtro estático.

Todo lo anterior es posible configurarlo en conjunto con el objetivo de otorgar un mejor control del acceso web, estos controles luego son asociados a perfiles definidos en los cuales se pueden otorgar horarios que se consideren necesarios para cada usuario o grupo de usuarios existentes.

4.3.3.7 IM&P2P

El control de estas aplicaciones se realiza en el equipo considerando los puertos TCP y UDP que estas utilizan para inicializar sus comunicaciones, sin embargo si es posible establecer el control de ellas, al configurar en el apartado de *Firewall / Advanced* en la sección de *Dynamic Ports* se habilita el soporte de MSN. Por otro lado es posible configurar grupos de servicios utilizando los servicios creados por defecto en el equipo, o incluso creando modificaciones a los servicios existentes con el fin de hacer más robusto el control sobre los aplicativos.

La configuración anterior es posible desde la sección *Firewall / Services* ya sea creando nuevos servicios en *Services* o asociando los existentes en *Services Groups*, en la figura 4.78 en donde se observan los grupos creados en base a los servicios existentes para efectos de prueba en el equipo.

Figura 4.78 Control de aplicaciones IM/P2P configurados

Luego se procedió a efectuar pruebas con los servicios creados aplicados en políticas de restricción de IM, P2P y VNC. Estas se efectuaron en horas de desempeño normales de la empresa, teniendo como resultado que el equipo si identifica el tipo de tráfico que se está generando en la red interna, sin embargo a la hora de denegar el acceso le resulta muy difícil, esto debido a que las políticas que se están utilizando para generar la acción están basadas en puertos definidos sobre los cuales se desenvuelven las aplicaciones, más sin embargo por las características de estas, son evadibles con facilidad. En la figura 4.79 se muestra el resultado de una captura de pantalla efectuado con un usuario de la red, en donde se observa que en un primer intento no se bloqueo el ni la aplicación VNC, ni el MSN, pero si el Yahoo Messenger.

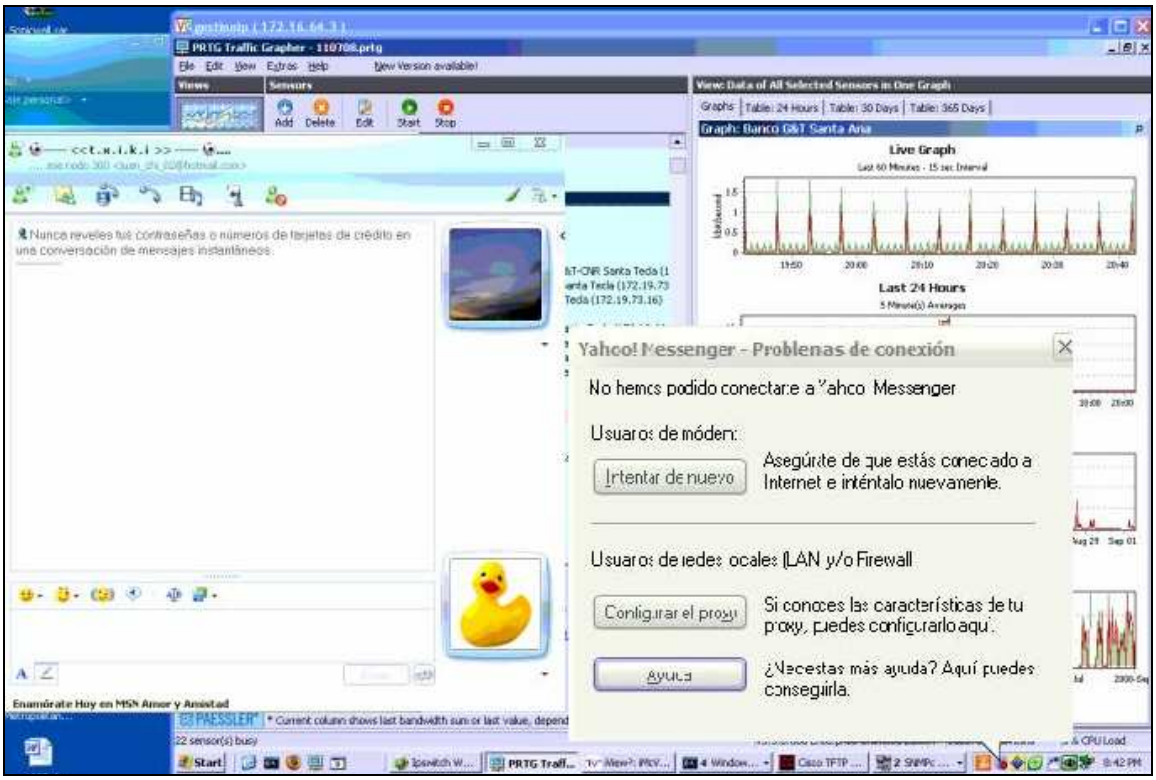


Figura 4.79 Ilustración de control de aplicaciones.

4.3.3.8 IPS

Para los sistemas IPS, se puede configurar la protección de estos desde el apartado *Security Services / □ortines□ Prevention* en donde se observa el estatus y la versión de la licencia. Además es de aclarar que por defecto los equipos no traen activa la protección IPS, de hecho una vez habilitados se debe de configurar las acciones que se desea el equipo realice, ya que estas vienen inhabilitadas, el equipo cuenta con tres categorizaciones las cuales en base al nivel de estas han agrupado firmas para mantener protegido o únicamente detectar las amenazas de ataques ya sean de alta prioridad, media prioridad o baja prioridad; esto se ilustra en la figura 4.80.

Figura 4.80 Sistema IPS

Por otro lado, se permite la creación de nuevos perfiles, en donde se puede activar el reensamblaje de paquetes a la hora de realizar la inspección, además de agregar listas de IP a las cuales no se analizaran en este perfil. Finalmente en la parte inferior se presentan las firmas que el equipo reconoce y con las cuales se pueden generar los nuevos perfiles de protección que el administrador del mismo considere convenientes. Lo anterior se ilustra en la figura 4.81.

Figura 4.81 Creación de nuevos perfiles IPS.

Es de aclarar que una vez habiendo definido los perfiles IPS a utilizar, es posible asignar estos a políticas o perfiles específicos para la identificación o protección de tráfico según sea necesario.

4.3.3.9 Antivirus.

La protección antivirus para este equipo se divide en dos apartados, la primera parte que se refiere a las licencias para usuarios finales que trae consigo el equipo, a las cuales se les pueden definir políticas específicas para los usuarios, así mismo definirles un tiempo como límite máximo antes de buscar actualizaciones o buscar estas una vez generada una alarma de alto riesgo, para ello se requiere de la instalación de un software en las PC a proteger. Esto es accesible desde la ubicación *Security Services / Client AV* y se presenta dicha ilustración en la figura 4.82

Figura 4.82 Configuración de Cliente AV.

Por otro lado, la protección antivirus perimetral se presenta en el apartado *Security Services / Gateway Antivirus*, en donde se puede observar la licencia utilizada y el estatus de la misma, por otro lado la protección perimetral de antivirus viene desactivada por defecto, el administrador deberá cambiar su estatus si desea activarlo, además es posible activarlo para la inspección en tipos de archivos de aplicativos específicos entre ellos están los http, FTP, IMAP, SMTP, POP3 y TCP Stream; esto se ilustra en la figura 4.83

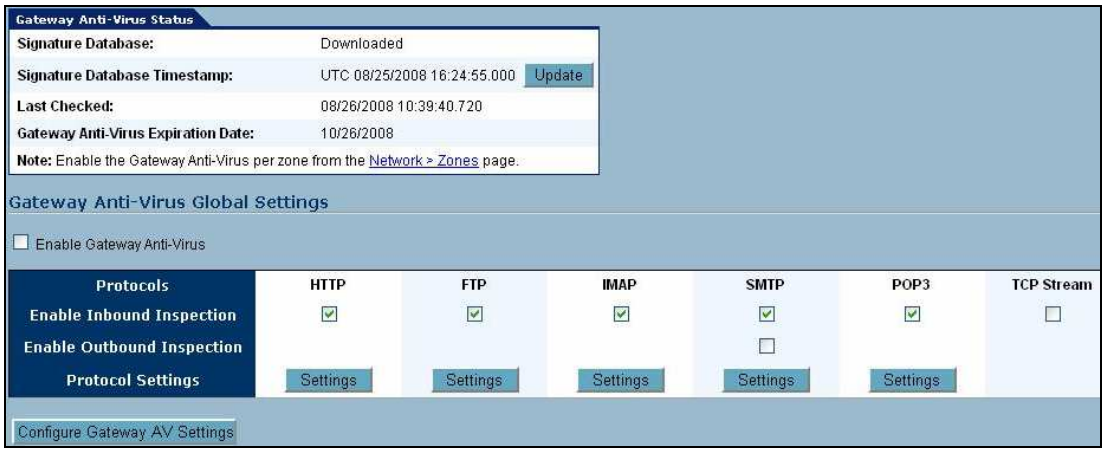


Figura 4.83 Configuración de Gateway Antivirus.

De la misma manera es posible la creación de listas de exclusión de análisis, así como las notificaciones de los archivos calificados como no confiables, dicho mensaje a mostrar es posible configurarlo utilizando HTML. Por otro lado, en este apartado se presentan las firmas que el dispositivo utiliza para el análisis de los archivos. En la figura 4.84 se presenta la ilustración de las firmas existentes en el equipo.

Figura 4.84 Firmas Antivirus.

4.3.3.10 Anti-Spyware

En el apartado de anti-spyware se presenta en primer plano la licencia utilizada y el estatus de la misma, luego se tiene la opción de habilitar el análisis antispyware en tres niveles configurados con la opción de prevenirlos y detectarlos, además de activar la inspección de entrada a los protocolos como http, FTP, IMAP, SMTP y POP3; además se tiene la opción de configurar la inspección de salida a este mismo conjunto de protocolos. En la figura 4.85 se presenta la ilustración de la ubicación *Security Services / Anti-Spyware*.

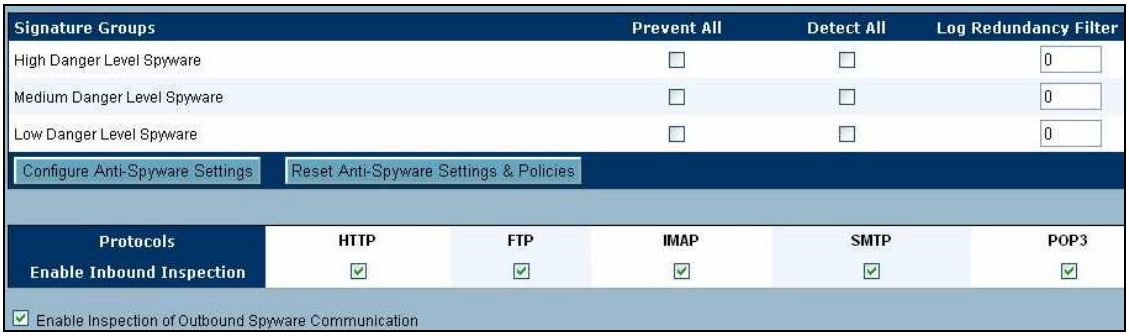


Figura 4.85 Configuración Anti-Spyware

Posteriormente se muestran las políticas que el equipo utiliza auxiliado por las firmas para determinar el nivel de severidad de las anomalías en cuanto a programas o aplicaciones espías se refiere. De la misma manera se da la opción para agregar alguna otra política que el usuario considere necesaria o modificar alguna de las ya existentes. En la figura 4.86 se muestra la ilustración de esto.

Figura 4.86 Nuevas políticas Anti-Spyware

4.3.3.11 Análisis de Correo

Para este apartado se presentan dos partes que son utilizadas para este fin en el equipo, primeramente se presenta el análisis de archivos adjuntos de correos electrónicos, el cual es accesible desde la ubicación *Security Services / E-Mail Filter*, como su nombre lo indica se utiliza para analizar los archivos adjuntos de los correos electrónicos, basándose en el listado de extensiones de archivos que el usuario desea analizar; posteriormente se presenta la configuración del mensaje que aparecerá en caso de detectarse alguna anomalía, en la última parte de esta ubicación existe la posibilidad de bloquear los fragmentos de correos SMTP. Lo anterior se ilustra en la figura 4.87

Figura 4.87 Análisis de Archivos Adjuntos.

La otra parte que se puede configurar para controlar el correo electrónico es el segmento de *Security Services / RBL filter* en donde se determinan por defecto dos servidores públicos con los cuales se consultara antes de aceptar cualquier correo proveniente de cualquier dominio, además se tiene la opción de configurar nuevos servidores en dicho apartado; por otro lado se pueden agregar usuarios a listas negras o listas blancas para el análisis o la restricción de los correos de estos. Esto se ilustra en la figura 4.88

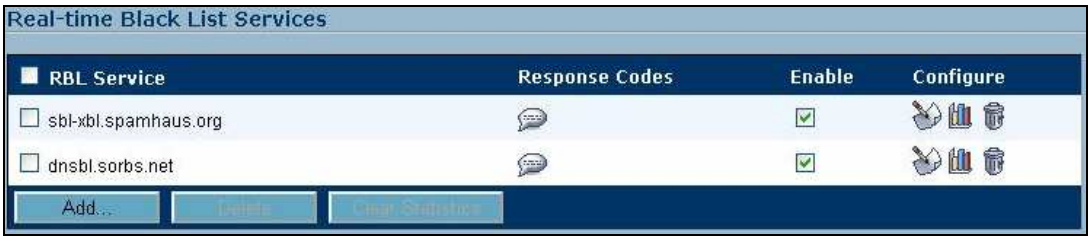


Figura 4.88 Análisis RBL de Emails.

4.3.3.12 Reportes

El dispositivo ofrece almacenamiento de logs incluso de algunos por ciertos periodos de tiempo de hasta un par de meses, de la misma manera es posible verificar logs del equipo en periodos de tiempo casi en tiempo real. En la ventana inicial del mismo, es decir desde la ubicación de System / Security Dashboard se puede visualizar estadísticas del desempaño en base al tipo de tráfico detectado en el dispositivo como por ejemplo http, P2P/IM, IPS o IDS. Estas estadísticas, se pueden visualizar en periodos de las últimas doce horas hasta periodos de los últimos seis meses, además de esto es posible la generación de una hoja en formato pdf con los datos antes mencionados que pudiesen utilizarse para tener una idea de la utilización del equipo. En la figura 4.89 se presentan las ilustraciones de las graficas antes mencionadas.

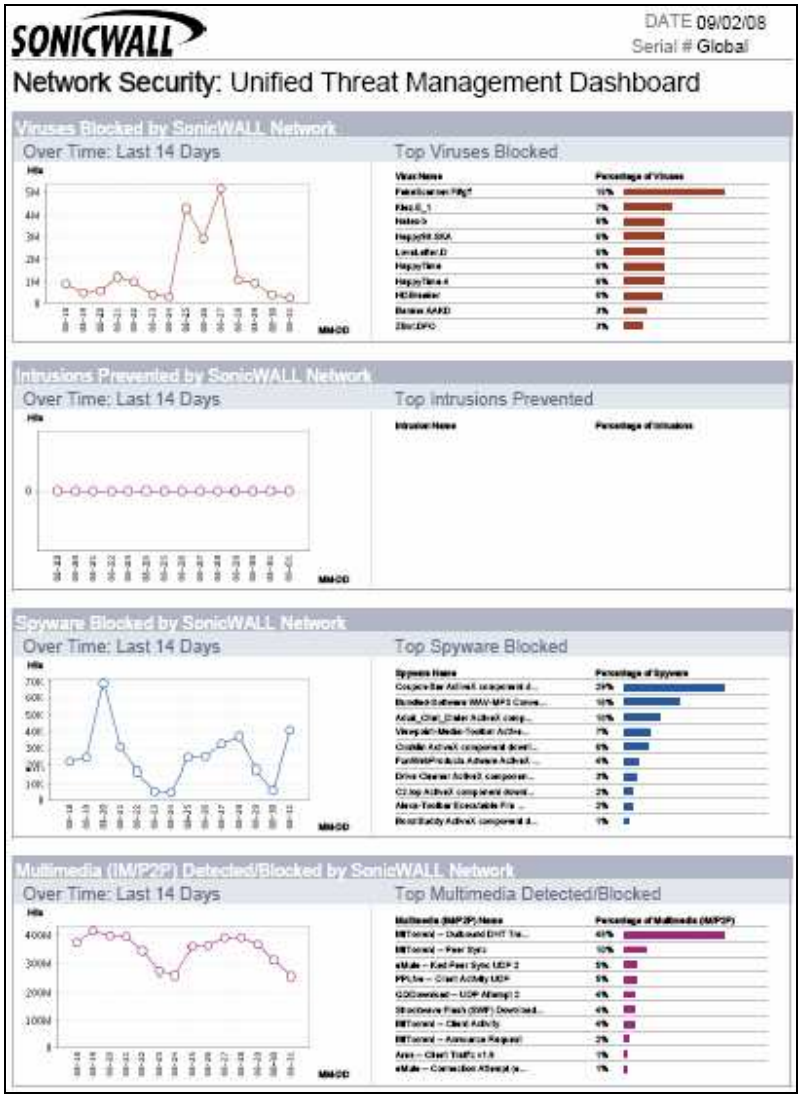


Figura 4.89 Reporte de estadísticas generado.

En el apartado de logs el equipo ofrece un segmento especializado en estos, permitiendo filtrar el tipo de log para tener una mejor visión del tipo de tráfico y eventos circulantes en el mismo; estos pueden ser filtrados dependiendo del tipo de evento generado, las interfaces involucradas o la categoría del mismo, posteriormente estos datos pueden ser exportados a un almacenador de logs como por ejemplo el syslog. La ilustración de esto se presenta en la figura 4.90 con los datos capturados durante las pruebas realizadas y es accesible desde la ubicación *Logs / View*.

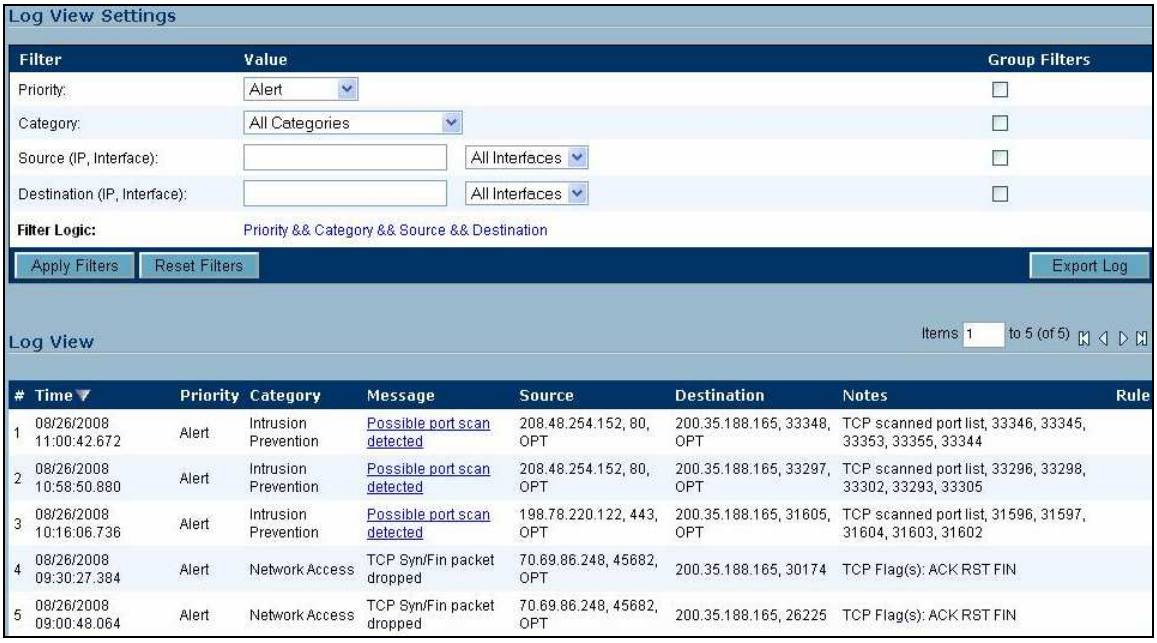


Figura 4.90 Ilustración del filtrado de Logs.

De la misma manera es posible la configuración del almacenamiento de logs en base a las categorías de estos, siendo posible realizarlo desde el apartado *Logs / Categories.* Pudiéndose configurar estos si pertenecen a categorías como emergencia, alerta, crítica, error, prevención, noticia o debug o de acuerdo a su nivel de alerta. También es posible el envío de estos logs o al menos de las alarmas más críticas por correo electrónico, esto se configura desde la ubicación *Logs / Autentication* en donde se le indica la cuenta de correo a la que se le enviara la notificación de la alarma.

El envío de logs hacia syslog también tiene su espacio en el equipo, sin embargo este no se realizo debido a que en primera instancia no se contaba con un servidor de este tipo y en segunda instancia, este equipo requiere de un agente externo para poder almacenar los logs en equipos externos.

Por otro lado, el dispositivo ofrece un apartado para la generación de reportes, esta es accesible desde la ubicación *Logs / Reports* en donde el usuario puede seleccionar los datos

que particularmente necesita, entre las estadísticas que el equipo puede manejar se pueden mencionar las veinticinco páginas web más visitadas, las IP's con mayor consumo de ancho de banda y los servicios que han utilizado mayor ancho de banda. En la figura 4.91 se presentan las ilustraciones respectivas.

Figura 4.91 Ilustración de reportes accesibles.

4.3.3.13 Wizards

El equipo ofrece la facilidad de contar con este apartado que es de mucha ayuda para el usuario que poca o nula relación ha tenido con este tipo de dispositivo, esta herramienta extra es en forma visual y muy sencilla de seguir paso a paso, se utilizaron estos para la configuración inicial del equipo, sin embargo luego de haber logrado el conocimiento del mismo se opto por realizar las configuraciones sin su ayuda ya que se logra más versatilidad en las configuraciones realizadas.

Se ofrecen cuatro wizards en el quipo la primera que está definida para la primera configuración del equipo ya sea que se configure en modo transparente o en modo routing, la segunda está definida para activar el registro y licencias del equipo útiles para el desempeño del mismo, el tercer wizard es utilizado para la configuración del switch usado para la LAN ya que puede ser segmentado en 2 o 4 aéreas lógicas diferentes, el cuarto apartado está definido para el uso o publicación de servidores públicos desde el segmento de LAN, finalmente el ultimo está diseñado para la configuración y creación de VPN punto a punto o de Gateway remoto. Esto es accesible desde la ubicación Wizards y se ilustra en la imagen 4.92.

Figura 4.92 Wizards.

4.4 Conclusiones de las Pruebas realizadas.

Primero se presentara una breve descripción de las comparaciones hechas entre ambos dispositivos y luego se visualizaran las tablas llenas resumiendo así los resultados de las pruebas realizadas.

Ambos equipos presentaban similitudes en un primer momento en cuanto a la interfaz grafica, así como a la versatilidad de aplicaciones, al desempeño y a la apariencia física de los mismos. Sin embargo después de un par de minutos de estar en contacto con cada uno, se puede observar muchas diferencias entre sí, desde diferentes apartados hasta simples cambios en la conceptualización de configuración. En la figura 4.93 se muestran las imágenes de los dispositivos sometidos a prueba, SonicWALL y Fortinet respectivamente. En el anexo 1 se presentan las hojas de especificaciones técnicas de estos equipos.

Figura 4.93 Equipos utilizados.

En la evaluación de equipo se inicio con el apartado de creación de perfiles, luego se evaluó la capacidad del equipo en agrupar IP's, autenticar usuarios, interconexión de los dispositivos con bases de datos externos, control de usuarios/políticas por horario, control de aplicativos, detección de códigos/archivos malicioso y la amigabilidad de la interfaz. En la tabla 4.4 se presenta las tablas generales de evaluación para ambos equipos.

Cuadro Comparativo de Dispositivos UTM											
	Firewall	Perfiles	IDS	IPS	Antivirus	Antispam	VPN	IM & P2P	Filtrado	Logs	Reportes
SONICWALL	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK
FORTINET	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	X

	Areas	NAT	HA	Throughput	RAM	VDOM	Consola	Interfaces	R. Dinamico
SONICWALL	1 - 5	OK	OK	90 M	128 M	X	OK	10	4
FORTINET	1 - 3	OK	OK	100 M	128 M	OK	OK	8	2

Tabla 4.4 Tablas generales de evaluaciones

En el primer cuadro, únicamente se colocan si el equipo según las especificaciones que se ofrecen cuenta con cada área evaluada. En el segundo cuadro, se presentan datos un tanto más específicos de las características de cada equipo, los cuales se describen a continuación:

- *Áreas:* muestra el número de segmentos lógicos en los que el equipo puede ser segmentado.
- *NAT:* si ofrece la opción de realizar NAT en su interior, un parámetro indispensable para este tipo de equipos.
- *HA:* alta disponibilidad, es decir si se puede colocar un par de estos equipos para que trabajen en conjunto para ofrecer redundancia o balanceo de trafico entre ellos.
- *Throughput:* la capacidad de procesamiento que tiene el microprocesador de cada equipo utilizado.
- *RAM:* la capacidad de memoria RAM con la que cuentan los dispositivos.
- *VDOM:* dominios virtuales, si los equipos ofrecen la característica de segmentarse a sí mismos en varios dispositivos lógicos ofreciendo así características específicas diversas según sean las necesidades.
- *Consola*: si ofrecen la posibilidad de realizar configuraciones desde la consola.
- *Interfaces:* muestran la cantidad de interfaces físicas con las que cuenta el equipo.
- *R. Dinámico:* muestra la cantidad de protocolos dinámicos que los equipos soportan.

Los resultados de cada apartado se presentaran con un cuadro obtenido según lo observado primero en la estructura del equipo y luego en el desempeño de los mismos. Es por esto que en las primeras dos columnas únicamente se indica si el dispositivo tiene la capacidad o cuenta con el modulo encargado de realizar una actividad en común, mientras que en la tercera columna se indica el equipo que presento mejores resultados en caso de haberse observado diferencias notables entre ambos. Luego en la parte inferior se presenta una breve explicación de lo expresado en las tablas respectivas.

4.4.1 Creación de perfiles.

Tabla de resultados obtenidos:

Versatilidad de creacion de perfiles

	SONICWALL	FORTINET	Superior
Agrupacion de IP's	OK	OK	
Autenticacion interna de usuarios	OK	OK	SONICWALL
Interconexion con bases de datos	OK	OK	FORTINET
Control por Horario / Fecha	OK	OK	FORTINET
Amigabilidad de Interfaz	OK	OK	

Tabla 4.5 Resultados obtenidos en la creación de perfiles.

En la evolución de equipo se inicio con el apartado de creación de perfiles, se evaluó la capacidad del equipo en agrupar IP’s, autenticar usuarios, Interconexión con bases de datos externos, control por horario y amigabilidad de la interfaz.

Es de mencionar que en esta evaluación ambos equipos tuvieron similares resultados, ya que al menos los puntos evaluados fueron cubiertos por estos, sin embargo en la última casilla de la tabla 4.5 se observa que el equipo SonicWALL presento ventajas en lo que se refiere a:

- *Autenticación interna de usuarios:* esto debido a que ofrece la versatilidad de creación de usuarios temporales con tiempo de vida definido, con la capacidad de auto desactivarse una vez cumplido el tiempo permitido ya que lleva una especie de conteo regresivo para la vida útil de estos, además de ofrecer la auto creación de perfiles y passwords aleatorios para estos mismos.

Por el otro lado, el equipo Fortinet presento ventajas en dos apartados:

- *Interconexión con bases de datos externas:* desde ambos equipos es posible esta configuración, sin embargo para interconectarse con bases de datos externas al equipo y lograr autenticación valida, SonicWALL requiere de un equipo intermediario para esto último; mientras que el equipo Fortinet ofrece las mismas ventajas de interconexión y autenticación con la simple instalación de un software en el servidor a interconectar además de ofrecer una mayor gama de dispositivos hacia los cuales es posible compartir información (Active Directory, LDAP, RADIUS o TACACS+).

- *Control por Horario/Fecha:* ambos equipos pueden realizar el control por horarios definidos, sin embargo el equipo Foritnet ofrece la ventaja de presentar dos secciones diferentes de horarios, una de un horario recursivo por días/ horas en la semana y la otra de un horario que sucede una única vez, por su lado SonicWALL ofrece únicamente el horario recursivo en días/horas de la semana.

4.4.2 Configuración de VPN

Tabla de resultados obtenidos:

Configuración de VPN

	SONICWALL	FORTINET	Superior
VPN SSL	X	OK	FORTINET
VPN IPSEC	OK	OK	FORTINET
VPN ' X '	OK	OK	
Interfaz de Configuracion	OK	OK	SONICWALL

Tabla 4.6 Resultados obtenidos en la configuración de VPN

En el segmento de VPN se tuvieron notables diferencias entre ambos, en parte debido a que el fabricante de SonicWALL ofrece un dispositivo especializado para la aplicación de VPN SSL, ventajas de dispositivos SonicWALL:

- *Interfaz de configuración*: ofreció una mejor ayuda al usuario inicial para la creación de las VPN con la utilización de los wizard diseñados para este apartado.

Cabe mencionar que ambos dispositivos presentaron la posibilidad de la creación de otra VPN que no había sido considerada con mayores datos en el documento, el equipo Fortinet posibilita la creación de VPN PPTP mientras que el dispositivo SonicWALL posibilita la creación de VPN L2TP.

El equipo Fortinet presentó la siguiente ventaja:

- *VPN SSL:* capaz de ser creadas bajo dos modalidades como una conexión de punto a punto usando dos dispositivos en cada extremo y la de usuario remoto que permite usando un solo equipo realizar conexiones desde sitios remotos únicamente utilizando un navegador con la IP publica del sitio central. El equipo SonicWALL no es capaz de realizar esta modalidad de VPN.

4.4.3 Web Filtering

Tabla de resultados obtenidos:

Web Filtering

	SONICWALL	FORTINET	Superior
Categorizacion de paginas web	OK	OK	FORTINET
Filtro por URL	OK	OK	
Filtro por palabras o frases	OK	OK	
Filtro de publicidad	OK	OK	
Filtro de Banners en paginas web	X	OK	FORTINET
Filtro de pop-up	OK	OK	SONICWALL
Listas Blancas	OK	OK	

Tabla 4.7 Resultados obtenidos de la configuración de Web Filtering.

En el apartado de Web Filtering se presentaron similitudes en cuanto a la posibilidad de creación de categorías web, filtrado por palabras o frases, filtrado de publicidad. La ventaja de SonicWALL fue la de ofrecer un acceso directo al bloqueo de ventanas pop-up.

Las ventajas del equipo Fortinet se describen a continuación:

- *Categorización de páginas web:* si bien es cierto, ambos equipos ofrecen la capacidad de control de tráfico web mediante categorizaciones dinámicas de páginas, sin embargo el equipo Fortinet ofrece la categorización web en grupos de segmentos definidos, los cuales a su vez se dividen en grupos más pequeños, ofreciendo en su totalidad un poco más de ochenta categorizaciones web, ofreciendo una mayor granularidad en el trato de estas, SonicWALL ofrece alrededor de 50 categorizaciones.

- *Filtro de banners en páginas web:* en este apartado, el equipo Fortinet ofrece la ventaja de bloquear los banners o áreas de páginas web restringidas o bloqueadas en el apartado de categorización web, las cuales se presentan en otras páginas web que no necesariamente estén dentro de las categorizaciones de estas.

4.4.4 P2P/IM

Tabla de resultados obtenidos:

IM & P2P			
	SONICWALL	FORTINET	Superior
Identificar Protocolos	OK	OK	
Cantidad de IM controlados	2	4	FORTINET
Cantidad de P2P controlados	3	6	FORTINET
Bloqueo de IM-P2P	OK	OK	FORTINET
Control de P2P	OK	OK	FORTINET
Control por cuentas de IM	X	OK	FORTINET
Control de aplicaciones sobre IM	X	OK	FORTINET

Tabla 4.8 Resultados obtenidos en la configuración de P2P/IM

La sección de IP/P2P presento similitudes en ambos equipos en las capacidades de identificar estos protocolos, bloquear y controlar estos aplicativos. Sin embargo el rango de desarrollo de Fortinet resulto ser mucho mayor y efectivo en las siguientes áreas:

- *Cantidad de IM controlados:* en el simple hecho de cuantificar los protocolos controlados, el equipo Fortinet ofrece manejar un número mayor de estos siendo capaz de controlar los aplicativos IM: ICQ, AIM, MSN y Yahoo messenger. Mientras que SonicWALL únicamente permite identificar los dos últimos aplicativos mencionados.

- *Bloqueo de IM/P2P:* el numero de aplicaciones IM controladas es mayor en Fortinet, además en las pruebas realizadas se demostró que además de ser este número superior, el control de aplicativos P2P e IM los realiza de una manera más efectiva esto debido a que por lo que se pudo apreciar el dispositivo SonicWALL únicamente controla estos aplicativos con los puertos iniciales de conexión de estos, que si bien es cierto bloquea un cierto número de usuarios, según lo comprobado alrededor del cincuenta a sesenta por ciento pero otros luego de un momento de retraso logran establecer y mantener la conexión sin problema alguno.

- *Control de P2P:* en el caso de Fortinet, este equipo además de ofrecer control para seis aplicativos diferentes: BitTorrent, eDonkey, Gnutella, Kazza, Skype, WinNY presentaba la posibilidad de controlar la cantidad de trafico que estos consumían, es decir se podía limitar la máxima tasa de transferencia para este tipo de tráfico y si a esto le agregamos que estos controles pueden ser añadidos a políticas con horarios o grupos de IP definidas hacer ver la versatilidad del equipo en esta área. Además cabe mencionar que este dispositivo es capaz de identificar los aplicativos que se desprenden

de los seis mencionados con anterioridad, por ejemplo el aplicativo eDonkey evoluciono en ciertas características dando paso a eMule, siendo también posible identificar y controlar a este aplicativo. Por otro lado SonicWALL ofrece la posibilidad de identificar algunos otros aplicativos P2P considerandolos como sistemas IPS, sin embargo estos no se incluyen en este apartado ya que no son catalogados como P2P sino como sistemas IPS.

- *Control por cuentas de IM:* un novedoso método de control para IM el que ofrece el equipo Fortinet, siendo este capaz de identificar la cuenta desde la cual se logea en el cliente de IM instalado en las maquinas de los usuarios de la red, una vez contando con el registro se puede permitir o denegar cuentas especificas evitando así que un simple cambio de IP o de PC solucione dicho control. Es de mencionar que la cuenta de IM tiene prioridad sobre el control realizado desde el segmento de control dinámico del equipo.

- *Control de Aplicaciones sobre IM:* además del control de registros antes mencionados, Fortinet ofrece la capacidad de controlar el tipo de trafico que pudiera llegar a circular en una ventana de IM, entre ellos tenemos el control de transferencia y la utilización de recursos como el audio o la voz que son comúnmente usados valiéndose de las versiones de IM que soportan estos extras.

4.4.5 IPS

Tabla de resultados obtenidos:

	IPS		
	SONICWALL	FORTINET	Plus
Identificacion de Amenazas	OK	OK	
Bloqueo Automatico de Amenazas	X	X	
Añadir listas blancas de protocolos	X	OK	FORTINET
Actualizacion automatica	OK	OK	

Tabla 4.9 Resultados obtenidos en configuración de IPS.

Ambos equipos presentaron similitudes en la identificación de amenazas, ya que se realizan en base a firmas específica que se actualizan de manera automática en un periodo determinado de tiempo. Por otro lado ambos dispositivos traen desactivada por defecto el apartado de bloquear las anomalías registradas, de hecho el cliente debe indicar el tipo de perfil o grupo que desea configurar por defecto para su protección, en ambos casos ya se contaba con grupos de firmas agrupados para que el administrador simplemente las aplicara

en los perfiles de su necesidad. El equipo Fortinet presento una ligera ventaja en el apartado:

- *Listas blancas de protocolos:* en este apartado Fortinet permite la configuración de grupos de firmas existentes o de firmas definidas por el administrador para que si estas se presentan en cualquier interfaz del equipo se tomen medidas de paso libre hacia el trafico identificado como tal, esto también es posible asignarlo en trafico proveniente de alguna IP en especifico.

4.4.6 Antivirus, Antispyware y Antispam.

Tabla de resultados obtenidos:

Antivirus - AntiSpam - AntiSpyware			
	SONICWALL	FORTINET	Plus
Deteccion de Spam-Virus	OK	OK	FORTINET
Bloqueo de Spam-Virus	OK	OK	FORTINET
Analisis de Archivos Adjuntos	OK	X	SONICWALL
Antispyware	OK	X	SONICWALL

Tabla 4.10 *Resultados obtenidos en configuración Antivirus-Antispyware-Antispam*

En el apartado de Antivirus y Antispam, los dos equipos presentan la capacidad de identificar y bloquear este tipo de tráfico no deseado. Sin embargo a continuación se presentan los apartados en los que Fortinet presento un cierto nivel de superioridad:

- *Detección de Spam-Virus:* en el apartado de antivirus, ambos equipos presentan el mismo perfil, identificando el trafico malicioso en base a firmas y patrones de tráfico; sin embargo Fortinet en el apartado de Antispam ofrece la posibilidad de configurar palabras o frases que se pueden identificar en el encabezado de los correos y en base a estos calificarlos como spam, lo mismo se puede hacer con el remitente.

- *Bloqueo de Spam-Virus:* una vez identificando el tipo de anomalía presentada, es posible la configuración del bloqueo o la permisión de estos, las cuales Fortinet en base a listas de palabras o expresiones pueden ser controlados.

Por otro lado SonicWALL presento ventajas en los apartados:

- *Analisis de archivos adjuntos:* capacidad observada únicamente en este fabricante de los dos comprobados, permitiendo examinar y evaluar extensiones definidas de

archivos, de la misma manera es posible el bloqueo de estos. Por otro lado es posible generar listas de exclusión en base a IP involucradas en el tráfico de mail.

- *Antispyware:* SonicWALL ofrece la capacidad de identificar y controlar este tipo de archivos maliciosos, definiendo los archivos en los cuales se pueden inspeccionar utilizando las firmas definidas para este fin.

4.4.7 Reportes

Tabla de resultados obtenidos:

Reportes			
	SONICWALL	FORTINET	Superior
Almacenamiento de Estadisticas	OK	OK	SONICWALL
Generacion de Reportes	OK	X	SONICWALL
Versatilidad de Reportes	OK	X	SONICWALL
Interconexion de logs	OK	OK	FORTINET

Tabla 4.11 Resultados obtenidos en configuración de reportes.

En el apartado de reportes, ambos equipos presentaban la capacidad de registrar y almacenar logs en su interior, sin embargo el rango de almacenamiento de estos es mucho mayor en el equipo SonicWALL, en gran medida a raíz de ello en dicho grupo evaluativo este mismo equipo fue el más ventajoso en las pruebas realizadas.

Con la excepción de la interconexión con bases de datos externas, que para el caso represento mayores facilidades el equipo Fortinet debido a que solo se necesitaba la instalación de un software en el servidor a interconectar para lograr comunicación entre ambos equipos, también presentaba una mayor cantidad de dispositivos hacia los cuales se podía realizar dicho intercambio de datos, proceso para el cual el equipo SonicWALL necesitaba de un dispositivo externo para lograr interconectar la autenticación entre ambos y representaba una menor cantidad de bases de datos con las que se podía interconectar.

En el equipo SonicWALL se percibieron las siguientes características ventajosas:

- *Almacenamiento de estadísticas:* el equipo permite el almacenamiento de estadísticas desde un tiempo máximo de seis meses, es un poco limitado en la visualización de los puntos específicos ya que solo da opción a elección de cuatro periodos, doce horas, catorce días, un mes y seis meses, pero si lo comparamos con Fortinet que no tiene posibilidad de visualizar estadísticas, se tiene una diferencia abismal entre ellos.

- *Generación de reportes:* similar a como sucedió con las VPN que el fabricante tenia a otro equipo especializado en la creación de ese aplicativo, lo mismo sucede con Fortinet que por sí mismo es limitada la posibilidad de crear reportes a partir de los logs almacenados ya que el fabricante tiene otro dispositivo especializado para la creación de reportes. Por su lado SonicWALL ofrece la capacidad de generar reportes por tipos de tráficos en cuatro periodos de tiempo definidos, así mismo es capaz de presentar las alarmas de eventos determinados o de IP's especificas, los cuales pueden ser exportados o enviados vía correo electrónico.

- *Versatilidad de Reportes:* el usuario puede delimitar al reporte del tipo de tráfico que requiere visualizar o el tipo de aplicativo en fechas determinadas. De la misma manera se presentan cuadros estadísticos con los servicios utilizados en fechas especificas, esto es de mucha utilidad para los administradores ya que se tiene acceso al historial de eventos que pudieron haber causado alguna anomalía en la red interna.

Se pudo observar que cada equipo de manera general cumple con lo ofertado a los clientes, sin embargo cada uno lo hace a su manera, en términos generales se puede decir que el equipo Fortigate es un tanto más sencillo en su configuración ya que la interfaz grafica es bastante intuitiva y su capacidad de segmentar aplicativos y usuarios es bastante granular, dos puntos muy importantes a la hora de elegir o preferir a un equipo determinado. Pudiéndose catalogar como un equipo de fácil configuración, muy granular y de muy buen desenvolvimiento en las aplicaciones que maneja.

Por otro lado SonicWALL es un tanto más complicado a la hora de su configuración, sin embargo permite realizar creación de perfiles, de políticas, de intrusiones nuevas en base a los servicios que están definidos o que se pueden definir de una manera más fácil, permitiendo así agregar más robustez a las políticas de dichos equipos. Por lo que se puede catalogar como un equipo diseñado para usuarios un tanto más conocedores en cuanto a servicios, protocolos, puertos y firmas.

V. CONCLUSIONES.

Luego de finalizar el trabajo de graduación se puede concluir que:

- Los sistemas de gestión unificadas de amenazas (UTM), se han convertido en un importante elemento para garantizar la protección perimetral de cualquier empresa por pequeña que esta sea. En lugar de aplicar varios elementos diferentes para lograr las diversas capas de protección para la parte de conexiones al exterior, resulta más eficaz, compacto, y con ello barato, colocar un solo elemento que agrupe la mayoría, o todas las funciones necesarias o al menos a las más importantes.

- Los UTM como dispositivos de seguridad periférica, tendrán control del tráfico entre la comunicación de las redes que utilicen como "pasarela" al dispositivo, sin embargo no es un dispositivo de usuario final, que pudiese regular o detectar las amenazas que son generadas desde dentro de la LAN; por ejemplo, si se tuviese un usuario con algún virus, malware o spyaware en dispositivos externos como CD, DVD, memoria SD, dispositivos USB, etc. y se llegase a infectar al host, el dispositivo UTM no funcionará como antivirus o antispyware para el host ya que la anomalía se genero desde dentro de la LAN, simplemente éste funcionara como limitador de tráfico, impidiendo que la red interna pudiese estar propagando anomalías a la red externa y registrando el segmento o host interno infectado.

- Si se desea contar con las últimas protecciones desarrolladas ante las amenazas más recientes, el dispositivo UTM requiere una conexión permanente a Internet con licencias válidas de actualización, puesto que la totalidad de estos dispositivos se actualizan periódicamente para estar al día con la protección periférica.

- Es de suma importancia la implementación de métodos de control granular de tráfico hacia Internet, principalmente cuando se tiene usuarios con diferentes niveles de conocimientos informáticos, beneficiando la administración y desempeño de una red informática.

- Es vital hacer del conocimiento de los posibles futuros usuarios, la necesidad de la actualización continua de las bases de datos de los dispositivos UTM, para que tomen en cuenta la caducidad de las licencias y la compatibilidad de ciertos modelos con las actualizaciones por lo menos para los siguientes cinco años.

- La utilidad que los equipos UTM pueden tener en el control de aplicativos informáticos, es permitir la creación de perfiles definidos para usuarios o grupos de usuarios creados según sean los requerimientos existentes, en horarios o fechas definidas y para aplicativos específicos, según sean las necesidades de la empresa, así como las funciones extras que estos pueden proporcionar.

- Los equipos UTM ofrecen similares aplicativos entre sí, sin embargo estos pueden variar en sus técnicas de identificación de tráfico, así como en sus diversos métodos para configurar dichos controles de tráfico y por consiguiente esto afecta en el desempeño de los equipos.

- De manera general un dispositivo UTM debe de contar al menos con las siguientes características:

  - Firewall
  - Filtrado de contenido web.
  - Creación de perfiles de usuarios.
  - Creación de VPN.
  - Control de amenazas (IDS, IPS, Antivirus, AntiSpyware).
  - Control de aplicaciones IM/P2P
  - Capacidad de generación de logs.

  Estas se verán afectadas según sea la técnica utilizada por cada equipo y la necesidad que se desea solventar, recordando que no es importante la capacidad de bloqueo a aplicaciones del equipo sino más bien la capacidad de control que se puedan ejercer sobre estas, así mismo como la granularidad con la que se cuente permitirá un mejor desempeño de los equipos en general.

VI. RECOMENDACIONES.

Al finalizar este trabajo de graduación, se recomienda que:

- Para futuros informes, se debe estudiar y comparar una mayor cantidad de equipos de diferentes marcas a nivel regional, para poder establecer un mayor rango de análisis entre estos equipos, y así, los usuarios utilicen esa investigación como referencia para tomar sus decisiones en la utilización de cierta marca dependiendo de sus necesidades.

- Para realizar una investigación más profunda con un mayor número de equipos, se debe contar con más tiempo para realizar las pruebas de los mismos, con el fin de poder ahondar y conocer las múltiples funciones que pueden desempeñar, desarrollando así un estudio más extensivo de estos equipos.

- Por lo que se pudo observar en los diversos apartados de los equipos utilizados y en los manuales de usuarios de los mismos, estos equipos son capaces de realizar aplicativos mucho más complejos que los comprobados en este documento, como por ejemplo establecer dominios virtuales (VDOMS), capacidad para crear y establecer nuevas firmas por parte del usuario, entre otras. Dichas funciones podrían ser de sumo interés para futuras investigaciones.

VII. BIBLIOGRAFIA Y FUENTES DE CONSULTA.

Documentos consultados:

Aquí se incluyen los documentos que han sido utilizados como fuente de consulta.

[1] Robert L. Ziegler, **"Firewall Linux Guía Avanzada"**, Prentice Hall 2da.edicion 1998.

[2] CheckPoint, **"Stateful Inspection"**, CheckPoint Software Tecnologies Agosto 2005.

[3] Raúl Siles Peláez, **"Análisis de seguridad e TCP/IP"**, O'Really & Associates 1ª. Edición Junio 2002.

[4] Juan Carlos Oré, **"Introducción a la Seguridad Informática"**, Presentacion expuesta Junio 2006.

[5] José María Morales Velázquez, **"Cortafuegos. Comparativas y Generaciones"**, Version 1.1 Programa de Postgrado de UNED 2003.

[6] Ben Rexworthy, **"Deep Packet Inspection"**, SecurityNet UK 2004.

[7] Allot Communications, **"Deep Packet Inspection"**, Allot Comunications 2007.

[8] Marcus Goncalves, **"Manual de Firewalls"**, Editorial McGraw-Hill 2004.

[9] Jorge Mieres, **"Los Falsos Malwares"**, ESET Latinoamerica Mayo 2007.

[10] Arturo Hernández, **"Virus Informático"**, Desarrollado en el Laboratorio de Interoperabilidad dela U.A.N.L 2006.

[11] Javier Portillo, **"Seguridad Informática"**, Editada por la Universidad de Madrid, Septiembre 2003.

[12] Nestor Martin, **"Seguridad en Redes"**, España 2004.

[13] Dr. Max, **"Nociones Básicas sobre P2P"**, Capitulo I, II, año 2008.

[14] Aaron Hackworth, **"Spyware"**, Produced by U.S.-CERT, año 2006.

[15] Panda Software, **"Spam"**, Produced by Panda Software, año 2006.

[16] José María Morales Vásquez, **"SSL y Otros Protocolos Seguros"**, Producido por la Universidad Politécnica de Madrid España, año 2005.

[17] Gabriel Verdejo, **"Seguridad en Redes IP"**, Documentos electrónicos desarrollados en España, año 2006.

[18] Nicholas Pappas, **"Network IDS & IPS Deployement Strategies"**, SANS Institute 2008.

Sitios Web consultados:

Sitios de los cuales se utilizo algún documento o información respectiva.

[1] Documento: **"Cortafuegos"**, Disponible en: www.arcet.gob.ar. Última fecha de consulta: abril 2008

[2] Documento: **"DPI"**, Disponible en: www.getadvanced.net. Última fecha de consulta: mayo 2008

[3] Documento: **"Deep Packet Inspection"**, Disponible en: www.security.net. Última fecha de consulta: mayo 2008

[4] Documento: **"Firewalls"**, Disponible en: www.sabia.tic.udc.es. Última fecha de consulta: abril 2008

[5] Documento: **"IPSec IPV4, IPV6"**, Disponible en: www.redes.linux.com. Última fecha de consulta: mayo 2008

[6] Documento: **"Firewall y Proxy"**, Disponible en: www.incoma.edu.ar. Última fecha de consulta: abril 2008

Sitios Web consultados de manera repetitiva:

Aquí se incluyen los sitios web consultados con más de un documento:

- Pagina web: "**Cisco"** Acceso: www.cisco.com
  Información consultada: Historia de los dispositivos de seguridad
  Principios Básicos de TCP/IP
  Utilidad de Firewalls y VPN

- Pagina web: "**Wikipedia"** Acceso: www.wikipedia.org
  Información consultada: Historia de dispositivos de seguridad UTM
  Definiciones Básicas
  Historia de P2P
  Glosario

- Página web: **"Fortinet"** Acceso: www.fortinet.com
  Información consultada: Descripción de elementos de un UTM
  Descripción de técnicas usadas por Fortinet
  Utilidades de Fotinet
  Aplicativos UTM.
  Especificaciones técnicas de equipo Fortinet.

- Pagina web: **"Sonicwall"** Acceso: www.sonicwall.com
  Información consultada: Descripción de elementos de un UTM
  Descripción de técnicas usadas por SonicWALL
  Utilidades de SonicWALL
  Aplicativos UTM.
  Especificaciones técnicas de equipo Sonicwall.

- Pagina web: **"Juniper"** Acceso: www.juniper.net
  Información consultada: Elementos de seguridad
  Métodos utilizados en seguridad de UTM.
  Aplicativos UTM.

- Pagina Web: **"Check Point"** Acceso: www.checkpoint.com
  Información consultada: Elementos de seguridad

Técnicas de seguridad en UTM
Aplicativos UTM.

- Pagina web: **“Barracuda”** Acceso: www.barracudanetworks.com
  Información consultada: Elementos de seguridad
  Aplicativos UTM.

VIII. GLOSARIO.

A.

Active Directory: es el término utilizado por Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores. Utiliza distintos protocolos (principalmente LDAP, DNS, DHCP, etc). Su estructura jerárquica permite mantener una serie de objetos relacionados con componentes de una red, como usuarios, grupos de usuarios, permisos y asignación de recursos y políticas de acceso

Advanced Encryption Standard (**AES**): también conocido como Rijndael, es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos. Se espera que sea usado en el mundo entero y analizado exhaustivamente, como fue el caso de su predecesor, el Data Encryption Standard (DES). El AES fue anunciado por el Instituto Nacional de Estandares y Tecnología (NIST) como FIPS PUB 197 de los Estados Unidos (FIPS 197) el 26 de noviembre de 2001 después de un proceso de estandarización que duró 5 años (véase proceso de Advanced Encryption Standard para más detalles). Se transformó en un estándar efectivo el 26 de mayo de 2002. Desde 2006, el AES es uno de los algoritmos más populares usados en criptografía simétrica.

Appliance: dispositivo en forma de hardware con software precargado generalmente propietario, en este caso se utilizara para describir a los dispositivos UTM, el usuario de estos rara vez tendrá acceso a la información del sistema operativo o a la modificación del mismo y únicamente se limitara a configurar dicho equipo de acuerdo a sus necesidades.

B.

Bat: son archivos de texto sin formato que contienen un conjunto de comandos DOS, estos son ejecutados en grupo de forma secuencial permitiendo automatizar diversas tareas.

Bittorrent: es un programa del tipo *peer-to-peer* desarrollado por Bram Cohen y *BitTorrent, Inc.*. Es usado para el intercambio de archivos entre usuarios mediante el protocolo BitTorrent. Desde el lanzamiento de la versión 6.0, dejó de ser de código abierto, siendo una versión modificada del cliente µTorrent.

Blowfish: es un codificador de bloques simétricos, diseñado por Bruce Schneier en 1993 e incluido en un gran número de conjuntos de codificadores y productos de cifrado. Mientras que ningún analizador de cifrados de Blowfish efectivo ha sido encontrado hoy en día, se ha dado más atención de la decodificación de bloques con bloques más grandes, como AES y Twofish.

C.

Cifrado: técnica de comunicaciones que tiene como principal objetivo el ocultar los datos que sobre ella se transmiten a personas o entidades no autorizadas para su información.

D.

Data Encryption Standard (DES): es un algoritmo de cifrado, es decir, un método para cifrar información, escogido como FIPS en los Estados Unidos en 1976, y cuyo uso se ha propagado ampliamente por todo el mundo. El algoritmo fue controvertido al principio, con algunos elementos de diseño clasificados, una longitud de clave relativamente corta, y las continuas sospechas sobre la existencia de alguna puerta trasera para la National Security Agency (NSA). Posteriormente DES fue sometido a un intenso análisis académico y motivó el concepto moderno del cifrado por bloques y su criptoanálisis.

DNS: Domain Name System es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

E.

Encapsulamiento: es el proceso por el cual los datos que se deben enviar a través de una red se deben colocar en paquetes que se puedan administrar y rastrear. Las tres capas superiores del modelo OSI (aplicación, presentación y sesión) preparan los datos para su transmisión creando un formato común para la transmisión.

eDonkey: es el nombre de una red de intercambio de archivos P2P, su nombre deriva del programa original creado para la misma. El nombre del cliente oficial es eDonkey2000, el cual en la actualidad ha dejado de funcionar. Dicho cliente tenía la capacidad de conectarse tanto a la red eDonkey como a Overnet.

eMule: es un programa para intercambio de archivos con sistema P2P utilizando el protocolo eDonkey 2000 y la red Kad, publicado como software libre para sistemas Microsoft Windows.

Ethernet: Ethernet es una tecnología de redes ampliamente aceptada con conexiones disponibles para PCs, estaciones de trabajo científicas y de alta desempeño, mini computadoras y sistemas mainframe.

F.

Falsos positivos: término aplicado a un fallo de detección en un sistema de alertas. Este término se aplica cuando se detecta la presencia de alguna anomalía en un sistema o equipo, la cual no existe.

Falsos negativos: término que hace referencia a un fallo en el sistema de alerta. Sucede cuando una anomalía está presente en nuestro sistema o equipo y este no logra identificarla o no se genera alerta en el sistema.

Fastethernet: también conocido como 10BASE-T, fue desarrollado en respuesta a la necesidad de una red LAN compatible con Ethernet con mayor tasa de transferencia que pudiera operar sobre el cableado UTP.

Firewall: es un elemento de en software o hardware utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red.

Firmas: en el ámbito de las redes informáticas, se define como el patrón de características de paquetería que sirve para identificar a una trama como parte de un tipo de tráfico en específico.

FTP: Abreviatura para 'File Transfer Protocol', es el protocolo usado en Internet para enviar archivos.

G.

Gigabit ethernet: también conocida como GigE, es una ampliación del estándar Ethernet que consigue una capacidad de transmisión de 1 gigabit por segundo, correspondientes a unos 1000 megabits por segundo de rendimiento contra unos 100 de Fast Ethernet.

Gnutella: es un proyecto de software distribuido para crear un protocolo de red de distribución de archivos entre pares, sin un servidor central.

H.

Hash: en informática, se refiere a una función o método para generar claves o llaves que representen de manera única a un documento, registro, archivo, etc, resumir o identificar un dato a través de la probabilidad obtenida de un algoritmo.

Heurística: es la capacidad de un sistema para realizar de forma inmediata innovaciones positivas para sus fines; es buscarle solución a los problemas de manera más intuitiva que

razonable basándose en la experiencia, reduciendo así el tiempo de solución de los problemas.

I.

IM: Instant menssenger. Programa aplicativo que requieren de un conjunto de programas que utilizan el protocolo TCP IP que sirven para enviar y recibir mensajes instantáneos con otros usuarios conectados a Internet u otras redes, además saber cuando están disponibles para hablar.

IMAP (Internet Message Access Protocol): protocolo de red de acceso a mensajes electrónicos almacenados en un servidor. Es decir usando este protocolo se puede tener acceso al correo electrónico desde cualquier host sin descargar el mail del servidor.

IP Spoofing: Es una técnica usada para obtener acceso no autorizado a las computadoras, en donde el 'intruso' envía mensajes a una computadora con una dirección IP indicando que el mensaje viene de una computadora confiable. Para lograr el IP Spoofing, un hacker debe primero de usar una variedad de técnicas para encontrar la dirección IP de una computadora confiable y posteriormente modificar el encabezado del paquete para que parezca que el paquete viene de esa computadora.

IRC: protocolo de comunicación en tiempo real basado en texto, que permite debates en grupo o entre dos personas y que generalmente se usa en la mensajería instantánea. Los usuarios de este protocolo utilizan una aplicación cliente para comunicarse con un servidor que gestiona los canales y las conversaciones.

ISP (proveedor de servicios de internet): es una empresa dedicada a conectar a Internet a los usuarios o las distintas redes que tengan, y dar el mantenimiento necesario para que el acceso funcione correctamente.

K.

Kazaa: es una aplicación para el intercambio de archivos entre pares que utiliza el protocolo Fast Track. Kazaa es comúnmente utilizado para intercambiar música (principalmente en formato mp3) y películas (en formato DivX). Su versión oficial puede ser descargada gratuitamente y su sustento económico es el spyware (software espía) y adware (software publicitario) instalado en forma predeterminada con el producto.

L.

LDAP (Lightweight Directory Access Protocol): es un protocolo de acceso unificado a un conjunto de información sobre una red. Habitualmente, almacena la información de login (usuario y contraseña) y es utilizado para autenticarse aunque es posible almacenar otra información

M.

MD5: (abreviatura de Message-Digest Algorithm 5, Algoritmo de Resumen del Mensaje 5) es un algoritmo de reducción criptográfico de 128 bits ampliamente usado.

N.

NAT (Network AddresTranslation): traducción de direcciones IP's, usado generalmente en equipos de borde de redes internas, este traducción puede ser estática entre una IP publica y otra privada, o puede ser dinámica una IP publica hacia varias privadas, a esto ultimo se le llama PAT.

P.

P2P: A grandes rasgos, una red informática entre iguales (en inglés, *peer-to-peer* -que se traduciría de par a par- o de punto a punto, y más conocida como P2P) se refiere a una red que no tiene clientes ni servidores fijos, sino una serie de nodos que se comportan simultáneamente como clientes y como servidores respecto de los demás nodos de la red. Es una forma legal de compartir archivos de forma similar a como se hace en el email o mensajeros instantáneos, sólo que de una forma más eficiente.

Paquete: un paquete es una pieza de un mensaje trasmitido. Una parte importante del paquete es que contiene la dirección destino, además de la información o datos. En redes IP, generalmente son llamados datagramas.

POP3 (Post Office Protocol) : protocolo utilizado en clientes locales de correo para obtener mensajes de correo electrónico almacenados en un servidor remoto, luego de obtenerlos estos son eliminados del servidor y el cliente los puede manipular sin problema alguno.

Protocolo: son lenguajes estándares, aceptados por la comunidad informática internacional que especifican cómo se deben de trocear los llamados paquetes de información.

Protocolo TCP/IP (Transport Control Protocol / Internet Protocol): protocolo surgido en los años sesentas como base de un sistema de comunicación basado en redes de

conmutación de paquetes desarrollado por el gobierno estadounidense y la agencia de defensa ARPA. Es el protocolo más usado para las comunicaciones electrónicas a través de Internet.

Proxy: hace referencia a un programa o dispositivo que realiza una acción en representación de otro, generalmente usado como equipo de borde.

R.

RADIUS: Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1813 UDP para establecer sus conexiones.

S.

Servidor Proxy: Es un servidor que se encuentra entre una aplicación cliente, por ejemplo un navegador de internet, y un servidor real. El servidor proxy intercepta todas las requisiciones que van al servidor para ver si el las puede cumplir, si no es así, le envía la requisición al servidor real.

SMTP (Simple Mail Transfer Protocol): protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras o dispositivos electrónicos. Está basado en el modelo cliente-servidor, donde un cliente envía un mensaje a uno o varios receptores.

Skype: es un software para realizar llamadas sobre Internet (VoIP), fundada en 2003 por los creadores de Kazaa. El código y protocolo de Skype permanecen cerrados y propietarios, pero los usuarios interesados pueden descargar gratuitamente la aplicación del sitio oficial. Los usuarios de Skype pueden hablar entre ellos gratuitamente.

SOAP: (siglas de Simple Object Access Protocol) es un protocolo estándar creado por Microsoft, IBM y otros, define cómo dos objetos en diferentes procesos pueden comunicarse por medio de intercambio de datos XML. Esto es una ventaja ya que facilita su lectura por parte de humanos, pero también es un inconveniente dado que los mensajes resultantes son más largos. SOAP es uno de los protocolos utilizados en los servicios Web.

SSH (Secure SHell): es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos, y también puede redirigir el tráfico de X para poder ejecutar programas gráficos si tenemos un Servidor X (en sistemas Unix) corriendo.

SHA: Secure Hash Algorithm, Algoritmo de Hash Seguro, es un sistema de funciones hash criptográficas relacionadas de la Agencia de Seguridad Nacional de los Estados Unidos y

publicadas por el National Institute of Standards and Technology (NIST). El primer miembro de la familia fue publicado en 1993 es oficialmente llamado SHA. Sin embargo, hoy día, no oficialmente se le llama SHA-0 para evitar confusiones con sus sucesores. Dos años más tarde el primer sucesor de SHA fue publicado con el nombre de SHA-1. Existen cuatro variantes más que se han publicado desde entonces cuyas diferencias se basan en un diseño algo modificado y rangos de salida incrementados: SHA-224, SHA-256, SHA-384, y SHA-512 (llamándose SHA-2 a todos ellos).

T.

TACACS (Terminal Access Controller Access Control System): es un protocolo de autenticación remota que se usa para comunicarse con un servidor de autenticación comúnmente usado en redes Unix. TACACS permite a un servidor de acceso remoto comunicarse con un servidor de autenticación para determinar si el usuario tiene acceso a la red

TCP: Abreviatura para 'Transmission Control Protocol'. TCP es uno de los protocolos principales para las redes tipo TCP/IP. En donde, el protocolo IP, lidia solamente con los paquetes y el TCP hace posible que dos computadoras establezcan la conexión e intercambio de información. TCP garantiza el envío de la información y también garantiza que los paquetes son entregados en el mismo orden en que fueron enviados.

Trama: es una unidad de envío de datos. Viene a ser sinónimo de paquete de datos o Paquete de red, aunque se aplica principalmente en los niveles OSI más bajos, especialmente en el Nivel de enlace de datos. Normalmente una trama constará de cabecera, datos y cola. En la cola suele estar algún chequeo de errores. En la cabecera habrá campos de control de protocolo.

Triple DES: En criptografía el Triple DES se llama al algoritmo que hace triple cifrado del DES. También es conocido como TDES o 3DES, fue desarrollado por IBM en 1978.

U.

UDP: Abreviatura para 'User Datagram Protocol', es un protocolo sin conexión, que, como TCP, corre encima de redes IP networks. A diferencia del TCP/IP, UDP/IP da muy pocos servicios de recuperación de errores, pero ofrece a cambio una manera directa de enviar y recibir datagramas sobre una red IP. Este protocolo es usado principalmente para transmitir mensajes sobre una red.

UTM (Unified Threaten Management): dispositivo de seguridad periférica usado para controlar el acceso, llevar registro y delimitar el tipo de trafico que se mueve desde/hacia una red interior hacia/desde una red exterior (Internet generalmente)

V.

VNC: es un programa de software libre basado en una estructura cliente-servidor el cual nos permite tomar el control del ordenador servidor remotamente a través de un ordenador cliente. También llamado software de escritorio remoto. VNC permite que el sistema operativo en cada computadora sea distinto: Es posible compartir la pantalla de una máquina de "cualquier" sistema operativo conectando desde cualquier otro ordenador o dispositivo que disponga de un cliente VNC portado.

X.

XML (sigla en ingles de *Extensible **M**arkup **L**anguage,o* lenguaje de marcas extensible): se propone como un estándar para el intercambio de información estructurada entre diferentes plataformas. Se puede usar en bases de datos, editores de texto, hojas de cálculo y casi cualquier cosa imaginable, no es realmente un lenguaje en particular, sino una manera de definir lenguajes para diferentes necesidades. Algunos de estos lenguajes que usan XML para su definición son XHTML, SVG, MathML.

IX. ANEXOS.

Anexo 1: Hojas Técnicas de los Equipos Utilizados.

FORTIGATE 100 A

Interfaces	
10/100 Ethernet ports	4
4-Port Switch	•
DMZ port	2
USB ports	2
System Performance	
Concurrent sessions	200,000
New sessions/second	4,000
Firewall throughput (Mbps)	100
168-bit Triple-DES throughput (Mbps)	40
Antivirus throughput* (Mbps)	8
Users	Unrestricted
Policies	1000
Schedules	256
Antivirus, Worm Detection & Removal	
Automatic virus database update from FortiProtect Network	•
Scans HTTP, FTP, SMTP, POP3, IMAP, and encrypted VPN Tunnels	•
Block by file size	•
Firewall Modes and Features	
NAT, PAT, Transparent (bridge)	•
Routing mode (RIP v1, v2)	•
Policy-based NAT	•
Virtual domains	2
VLAN tagging (802.1q)	•
User Group-based authentication	•
H.323 NAT Traversal	•
WINS support	•
VPN	
PPTP, L2TP, and IPSec	•
Dedicated tunnels	80
Encryption (DES, 3DES, AES)	•
SHA-1 / MD5 authentication	•
PPTP, L2TP, VPN client pass though	•
Hub and Spoke VPN support	•
IKE certificate authentication	•
IPSec NAT Traversal	•
Dead peer detection	•
Content Filtering	
URL/keyword/phrase block	•
URL Exempt List	•
Protection profiles	32
Blocks Java Applet, Cookies, Active X	•
FortiGuard™ web filtering support	•
Dynamic Intrusion Detection and Prevention	
Intrusion prevention for over 1300 attacks	•
Automatic real-time updates from FortiProtect Network	•
Customizable detection signature list	•
Anti-Spam	
Real-time Blacklist/Open Relay Database Server	•
MIME header check	•
Keyword/phrase filtering	•
IP address blacklist/exempt list	•

Logging/Monitoring	
Log to remote Syslog/WELF server	•
Graphical real-time and historical monitoring	•
SNMP	•
Email notification of viruses and attacks	•
VPN tunnel monitor	•
Networking	
Multiple WAN link support	•
Multi-zone support	•
Route between zones	•
Policy-based routing	•
System Management	
Console interface	•
WebUI (HTTPS)	•
Multi-language support	•
Command line interface	•
Secure Command Shell (SSH)	•
FortiManager System	•
Administration	
Role-based administration	•
Multiple administrators and user levels	•
Upgrades & changes via TFTP & WebUI	•
System software rollback	•
User Authentication	
Internal database	•
External LDAP/RADIUS database support	•
RSA SecurID	•
Xauth over RADIUS support for IPSec VPN	•
IP/MAC address binding	•
Traffic Management	
DiffServ setting	•
Policy-based traffic shaping	•
Guaranteed/Maximum/Priority bandwidth	•
Dimensions	
Height	1.75 inches
Width	12.6 inches
Length	6.13 inches
Weight	7.3 lb (3.3 kg)
Power	
DC input voltage	12V
DC input current	5A
External power supply	100 to 240VAC
Environmental	
Operating Temperature	32 to 104 °F (0 to 40 °C)
Storage Temperature	-13 to 158 °F (-25 to 70 °C)
Humidity	5 to 95% non-condensing
Compliance	
FCC Class A Part 15, CE, UL, CUL, VCCI, C-Tick, CB	•
ICSA Antivirus, Firewall, IPSec, NIDS	•

SonicWALL TZ 190

SonicWALL TZ 190

Cortafuegos

Nodos admitidos	Ilimitados
Rendimiento de paquetes dinámicos	90 Mbps y superior
Rendimiento de Gateway Anti-Virus	10 Mbps
Rendimiento de Intrusion Prevention	8 Mbps
Rendimiento de Gateway Anti-Spyware	6 Mbps
Conexiones	6.000
Políticas	250 por zona
Protección contra denegación de servicio	22 clases de ataques DoS, DDoS y de escaneo

VPN

Rendimiento 3DES	30 Mbps y superior
Rendimiento AES	30 Mbps y superior
VPN entre emplazamientos	15 túneles máx.
VPN de acceso remoto	Ampliable a 25 usuarios simultáneos, incluye 2 licencias
Cifrado	DES, 3DES, AES (128, 192, 256)
Autenticación	MD5, SHA-1
Intercambio de claves	IKE, clave manual, certificados (X.509)
XAUTH/RADIUS	Sí
L2TP/IPSec	Sí
Dead Peer Detection	Sí
DHCP a través de VPN	Sí
IPSec NAT Traversal	Sí
Pasarela VPN redundante	Sí

Servicios de seguridad de inspección profunda

Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention	Amplia base de datos de definiciones de virus. Control de aplicaciones punto a punto y de mensajería instantánea, así como actualización de definiciones mediante arquitectura de refuerzo distribuido a través de todas las interfaces
Content Filtering Service (CFS)	Rastreo por URL, palabra clave y contenido, bloqueo de ActiveX®, Java Applets y cookies
Antivirus de red reforzado en pasarela	HTTP/S, SMTP, POP3, IMAP y FTP, cliente McAfee™ reforzado, bloqueo de anexos de correo electrónico
Paquete de prestaciones	90 días 8x5 o actualizaciones de software y firmware. Clientes Global VPN y servicios según se describen arriba

LAN inalámbrica

Controlador de LAN inalámbrica	Incluido
Versiones de SonicPoint	802.11a/b/g y 802.11b/g
SonicPoints gestionados	Como máximo 8 por interfaz, 16 por dispositivo
Normas WLAN	IEEE 802.11a, 802.11b, 802.11g, 802.11d, 802.11i (Requiere SonicOS Enhanced 3.7 o superior)
Alimentación por Ethernet (PoE)	SonicPoints admiten 802.3af PoE
Seguridad WLAN	WPA, WEP 64/128/152 de bits, TKIP, AES, 802.11i (Requiere SonicOS Enhanced 3.7 o superior)

WAN inalámbrica 3G

Indicador de fuerza de la señal inalámbrica	LED (velocidad variable) e interfaz gráfica de usuario
Tarjetas de PC soportadas*	Novatel Wireless Merlin PC720/ Novatel Wireless Merlin S620 (Tarjeta Sprint de banda ancha móvil) Novatel Wireless Merlin S720 (Tarjeta Sprint de banda ancha móvil) Novatel Wireless Merlin V620 Option GlobeTrotter GT MAX Option GlobeTrotter GT MAX 7.2 ready Option GlobeTrotter HSDPA Option GT Max 3.6 Sierra Wireless AirCard 860

Rendimiento WWAN típico**	
EV-DO rev A	1.000 a 2.000 kbps
EV-DO	400 a 700 kbps
1xRTT	80 a 100 kbps
HSDPA	1.000 a 2.000 kbps
UMTS	300 a 500 kbps
EDGE	200 a 400 kbps
GPRS	80 a 100 kbps
Informes sobre el uso del ancho de banda	Estadísticas del tráfico cargado y descargado diarias, semanales, mensuales y anuales
Alerta de inserción/ retirada de tarjeta	Las alertas se envían a través de la interfaz WAN por cable al administrador remoto o al Sistema de Gestión Global
Gestión del ancho de banda en la WWAN	FIFO, CBQ, RFC 2309, regulación por interfaz y por acceso; ancho de banda garantizado, ancho de banda máximo, prioridad

LAN

Interfaces LAN	(8) 10/100 Ethernet
PortShield	Un máximo de ocho zonas de seguridad personalizadas
Velocidad puerto	10 Mbps, 100 Mbps, Automática, Desactivada
Dúplex	Total, Media, Automática
Estadísticas de tráfico	Recuento de bytes transmitidos/recibidos, TX/RX

Conexión a red

DHCP	Servidor interno, relé
Modos NAT	1:1, muchos:1, 1:muchos, muchos:muchos, NAT flexible, PAT
Enrutamiento por políticas	Decisiones de enrutamiento basadas en combinaciones de IP de origen, IP de destino y servicio
Modos WAN	Modos NAT y transparente con direccionamiento estático o dinámico
Soporte DDNS	dyndns.org, yi.org, no-ip.com y change-ip.com
Autenticación	RADIUS, LDAP, AD, bases de datos internas (máx. 150 usuarios)

Hardware

Interfaces	(8) 10/100 LAN, (1) 10/100 WAN, (1) 10/100 OPT
Memoria (RAM)	128 MB
Flash	16 MB
Potencia de entrada	100 a 240 V CA, 50-60 Hz, 1 A
Consumo eléctrico máximo	12,7 W
Calor disipado total	43,3 BTU
MTBF	9,6 años
Certificaciones (pendientes)	ICSA Firewall 4.1, ICSA IPSec VPN 1.0d, FIPS 140-2, VPNC AES, Criterios Comunes EAL-2
Dimensiones	25,4 x 17,8 x 3,0 cm 10,0 x 7,0 x 1,2 pulgadas
Peso	0,92 kg 2,0 libras
Peso de suministro	2,1 kg 4,75 libras
Peso DEEE (Desperdicios de equipos eléctricos y electrónicos)	1,3 kg 2,75 libras
Conformidad con normas	FCC Class B, ICES Class B, CE, C-Tick, VCCI Class B, NOM, UL, cUL, TÜV/GS, CB, RoHS, DEEE
Entorno	5-40° C (40-105° F)
Humedad	10-90% sin condensación

* Para obtener una lista completa de las tarjetas soportadas, consulte nuestra página: http://www.sonicwall.com/us/tz190cards.html

**El rendimiento real depende de diversos factores, entre ellos la proximidad a la torre celular, las condiciones meteorológicas y la cantidad de tráfico de red. Además, el gráfico muestra el rendimiento en régimen de descarga. El rendimiento en régimen de carga es menor.