ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN TECNOLÓGICA

DISEÑO E IMPLEMENTACIÓN DE UNA RED SEGURA PARA EL LABORATORIO DE TECNOLOGÍAS DE LA INFORMACIÓN

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE TECNÓLOGO EN ANÁLISIS DE SISTEMAS INFORMÁTICOS

CARINA PATRICIA FIALLOS FIALLOS
SUSANA ALEJANDRINA TORO ROMERO

DIRECTOR: ING. FABIO GONZÁLEZ

Quito, Abril 2007

DECLARACIÓN

Nosotras, Carina Patricia Fiallos Fiallos, Susana Alejandrina Toro Romero, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Carina Patricia Fiallos Fiallos

Susana Alejandrina Toro Romero

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Carina Patricia Fiallos Fiallos, Susana Alejandrina Toro Romero, bajo mi supervisión.

Ing. Fabio González
DIRECTOR DE PROYECTO

AGRADECIMIENTO

Queremos exteriorizar nuestra gratitud imperecedera a todos nuestros profesores, por la oportunidad de habernos realizado profesionalmente acrecentando nuestro acervo intelectual. Especialmente al Ing. Fabio González, Ing. César Gallardo e Ing. Daniel Manangón, que en forma desinteresada nos ayudaron a llevar a feliz término la realización de este proyecto.

De manera muy especial al Ing. Víctor Ulloa, quién nos brindó las facilidades necesarias para el desarrollo de la presente investigación.

Y a nuestros amigos que de alguna manera contribuyeron con sus sabios consejos y recomendaciones, demostrándonos su amistad en todas las circunstancias a lo largo de nuestra etapa universitaria.

Carina Fiallos Fiallos

Susana Toro Romero

DEDICATORIA

A mi madre en virtud a una mujer de entrega, constancia y fortaleza. Poseedora de un gran espíritu y un inmenso corazón. Por incentivarme a soñar y a luchar para hacerlo realidad. Por grabar en mi alma su maravillosa frase “Quien tiene a Dios lo tiene todo”.

A mi padre por brindarme su cariño, confianza y dedicación. Por guiarme por el sendero de la honestidad y la sencillez.

A mis hermanas por su constante ayuda y su cariño incondicional. Por apoyarme y compartir conmigo los mejores momentos de mi vida.

Carina Fiallos Fiallos

DEDICATORIA

Al recuerdo imborrable de mi padre, que desde la diestra del Señor ha sabido guiar mi camino y ha sido mi mayor inspiración de superación y perseverancia.

A mi abnegada madre, a quien le debo todo lo que soy. Por su cariño y apoyo incondicional, quién con su ejemplo de trabajo, sacrificio y constancia me ha dado la fortaleza para seguir adelante. Por lo cual se ha ganado mi mayor admiración y respeto.

A mi hermano, quien me ha incentivado a luchar por lograr mis objetivos y no desmayar.

A Xavier E., por toda la confianza que ha depositado en mí, por su cariño sincero, su paciencia y comprensión, por sus sabios consejos y enseñanzas que me ayudaron a crecer como persona y como profesional.

Susana Toro Romero

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPITULO I

GENERALIDADES

INTRODUCCIÓN

Actualmente, Internet se compone de decenas de miles de redes conectadas entre si. La seguridad en las redes resulta esencial en este entorno, ya que toda red organizada es accesible desde cualquier computadora de la red y, potencialmente es vulnerable a las amenazas de personas que no necesitan acceso físico a ella.

La seguridad es una de las preocupaciones principales del administrador de red, debido a que en la actualidad los peligros de ataques y virus informáticos son muchos y variados, y casi diariamente aparecen nuevas técnicas e imaginativos ataques que pueden explotar un sistema mal protegido. Así pues, es necesario desarrollar un sistema que proteja a la red interna de la otra red, la Internet, mediante el uso de filtros equipados para evitar automáticamente que un usuario no-autorizado ataque al equipo. Lo recomendable es, además de un programa antivirus, disponer de un buen Firewall.

1.1 GENERALIDADES

1.1.1 INTRUSOS

1.1.1.1 Troyano[1]

Es un programa simple que facilita el control remoto de un computador, también denominados "malware" y realmente no son más que aplicaciones de gestión remota, que por ser totalmente gratuitos están muy difundidos y suelen utilizarse para el acceso a otros computadores de la red sin el debido permiso.

1.1.1.2 Hacker[2]

Este término normalmente es utilizado para identificar a una persona que únicamente accede a un sistema protegido sin intentar causar daños.

1.1.1.3 Cracker[3]

Su principal objetivo es producir daños que en muchos casos suponen un problema de extrema gravedad para el administrador del sistema.

1.1.1.4 Piratas

Su actividad se centra en la obtención de información confidencial y software de manera ilícita.

1.1.1.5 Virus Informáticos[4]

Los virus informáticos son programas que se introducen de forma oculta en un computador para ejecutar en él acciones no deseadas por sus usuarios habituales. La definición más simple y completa que hay de los virus se

---

[1] http://es.wikipedia.org/wiki/Troyano_(inform%C3%A1tica)
[2] http://es.wikipedia.org/wiki/Hacker
[3] http://es.wikipedia.org/wiki/Cracker
[4] http://es.wikipedia.org/wiki/Virus_inform%C3%A1ticos

fundamenta en tres características, que se refuerzan y dependen mutuamente: Dañino, Auto-reproductor, Subrepticio*, que corresponden al modelo D.A.S.*

Tienen diferentes finalidades: Algunos sólo 'infectan', otros alteran datos, otros los eliminan, algunos sólo muestran mensajes. Pero el fin último de todos ellos es el mismo: *propagarse***.**

Es importante destacar que el potencial del daño de un virus informático no depende de su complejidad pero si del entorno donde actúa.

Se pueden distinguir tres módulos principales de un virus informático:

- Módulo de Reproducción
- Módulo de Ataque
- Módulo de Defensa

1.1.1.5.1 El Módulo de Reproducción

Se encarga de manejar las rutinas de "parasitación" de entidades ejecutables (o archivos de datos, en el caso de los virus macro) a fin de que el virus pueda ejecutarse discretamente. Pudiendo, de esta manera, tomar control del sistema e infectar otras entidades permitiendo se traslade de una computadora a otra a través de algunos de estos archivos.

1.1.1.5.2 El Módulo de Ataque

Es optativo y está encargado de manejar las rutinas de daño adicional del virus. Por ejemplo, existen virus que además de producir daños muy pronunciados, tiene un módulo de ataque que se activa cuando el reloj de la computadora indica una fecha determinada. En estas condiciones la rutina actúa sobre la información del disco duro volviéndola inutilizable.

1.1.1.5.3 El Módulo de Defensa

Tiene la misión de proteger al virus y, como el módulo de ataque, puede estar o no presente en la estructura. Sus rutinas apuntan a evitar todo aquello que provoque la eliminación del virus y retardar su detección.

Los Virus pueden causar los siguientes daños:

En el Software

- Modificación de programas para que dejen de funcionar.
- Modificación de programas para que funcionen erróneamente.
- Modificación sobre los datos.
- Eliminación de programas y/o datos.
- Hacer que el sistema funcione más lentamente.
- Acabar con el espacio libre en el disco duro.

En el Hardware

- Borrado del BIOS.

Formas de propagación de los virus

- Memoria Flash u otro medio de almacenamiento removible
- Redes de computadoras
- Mensajes de correo electrónico
- Software descargado de Internet

Síntomas que indican la presencia de virus

- Cambios en la longitud de los programas
- Cambios en la fecha y/u hora de los archivos
- Retardos al cargar un programa
- Operación más lenta del sistema
- Reducción de la capacidad en memoria y/o disco duro
- Sectores defectuosos en los disquetes
- Mensajes de error inusuales

- Actividad extraña en la pantalla
- Fallas en la ejecución de los programas
- Fallas al reiniciar el equipo
- Escrituras fuera de tiempo en el disco

1.1.2 TIPOS DE VIRUS DE COMPUTACIÓN POR SUS ACCIONES Y/O MODO DE ACTIVACIÓN[5]

1.1.2.1 Bombas

Se activan segundos después de verse el sistema infectado o después de un cierto tiempo (bombas de tiempo) o al comprobarse cierto tipo de condición lógica del equipo (bombas lógicas). Ejemplos de bombas de tiempo son los virus que se activan en una fecha u hora determinada. Ejemplos de bombas lógicas son los virus que se activan cuando al disco duro solo le queda el 10% sin uso, etc.

1.1.2.2 Camaleones

Son una variedad de virus similares a los caballos de Troya. Cuando están correctamente programados, los camaleones pueden realizar todas las funciones de los programas legítimos a los que sustituyen (actúan como programas de demostración de productos, los cuales son simulaciones de programas reales). Un software camaleón podría, por ejemplo, provocar un conflicto a un programa de acceso a sistemas remotos realizando todas las acciones que ellos realizan, pero como tarea adicional (y oculta a los usuarios) va almacenando en algún archivo los diferentes logins y passwords para que posteriormente puedan ser recuperados y utilizados ilegalmente por el creador del virus camaleón.

1.1.2.3 Reproductores

Se reproducen en forma constante una vez que son ejecutados hasta agotar totalmente el espacio de disco o memoria del sistema. La única función de este

---

[5] http://www.monografias.com/trabajos15/virus-informatico/virus-informatico.shtml

tipo de virus es crear clones y lanzarlos a ejecutar para que ellos hagan lo mismo. El propósito es agotar los recursos del sistema, especialmente en un entorno multiusuario interconectado, hasta el punto que el sistema principal no puede continuar con el procesamiento normal.

1.1.2.4 Gusanos (Worms)

Son programas que constantemente viajan a través de un sistema informático interconectado, sin dañar necesariamente el hardware o el software de los sistemas que visitan. La función principal es viajar en secreto a través de equipos anfitriones recopilando cierto tipo de información programada (tal como los archivos de passwords) para enviarla a un equipo determinado al cual el creador del virus tiene acceso.

1.1.2.5 Backdoors

Son programas que permiten controlar remotamente la PC infectada. Generalmente son distribuidos como troyanos. Cuando un virus de estos es ejecutado, se instala dentro del sistema operativo, al cual monitorea sin ningún tipo de mensaje o consulta al usuario. Incluso no se lo vé en la lista de programas activos. Los Backdoors permiten al autor tomar total control de la PC infectada y de esta forma enviar, recibir, borrar o modificar los archivos, etc.

1.1.3 UNA NUEVA CLASIFICACIÓN DE VIRUS[6]

De acuerdo a la funcionalidad de ciertos virus un usuario puede tomar las debidas precauciones como por ejemplo:

1.1.3.1 Virus en archivos "fantasmas"

Estos virus basan su principio en que DOS, al tener dos archivos con el mismo nombre, ejecuta primero el archivo COM y luego el EXE, siempre y cuando estos

[6] http://www.monografias.com/trabajos17/virus-informaticos/virus-informaticos.shtml#nueva

archivos se encuentren en el mismo directorio. Al infectar la computadora, el virus crea un archivo COM con el mismo nombre y en el mismo lugar que el EXE a infectar. De este modo, se asegura que durante la próxima ejecución, el sistema operativo arrancará el nuevo archivo COM creado por el virus y conteniendo el código viral, para luego ceder el control al archivo EXE.

1.1.3.2 Virus de boot sector o sector de arranque

Infectan el sector de booteo o arranque de discos duros o diskettes. Las PC se infectan cuando se arranca el equipo con el diskette infectado, siempre y cuando el setup de la PC esté programado para arrancar primero desde el drive A:. Si por el contrario el setup inicia primero desde el disco duro, no es necesario preocuparse por este tipo de virus.

1.1.3.3 Virus de archivos ejecutables

Infectan los archivos que la PC toma como programas: *.EXE, *.DRV, *.DLL, *.BIN, *.OVL, *.SYS e incluso BAT. Pueden permanecer residentes en memoria durante mucho tiempo después de haber sido activados, en ese caso se dice que son virus residentes, o pueden ser virus de acción directa, que evitan quedar residentes en memoria y se replican o actúan contra el sistema sólo al ser ejecutado el programa infectado. Se dice que estos virus son virus de sobreescritura, ya que corrompen al fichero donde se ubican.

1.1.3.4 "Virus" Bug-Ware

Son programas que en absoluto no son virus informáticos, sino fragmentos de código mal implementado, que debido a fallos lógicos, dañan el hardware o inutilizan los datos del computador. En realidad son programas con errores, pero funcionalmente el resultado es semejante al de los virus.

1.1.3.5 Virus de Macro

Los virus macro se esparcen fácilmente a través de archivos adjuntos de e-mails, disquetes, programas obtenidos en Internet, transferencia de archivos y aplicaciones compartidas. Algunas macros son tan potentes que deben considerarse instrucciones de programación. Las macros del paquete Office, son en realidad un subconjunto de instrucciones de Visual Basic y son muy fáciles de crear. Pueden infectar diferentes puntos de un archivo en uso, por ejemplo, cuando éste se abre, se graba, se cierra o se borra. Este tipo de virus se activa al abrir un archivo infectado dentro del procesador de texto.

1.1.3.6 Virus de e-mail

Dentro de este grupo, se incluyen dos tipos de virus: los que junto a un mail hacen llegar un archivo adjunto que necesariamente debe abrirse o ejecutarse para activar el virus, y también están los gusanos (worms) que aprovechan los agujeros de seguridad de programas de correo electrónico para infectar a las computadoras. Esta variedad difiere de los otros virus en el hecho de que no necesitan de la ejecución de un programa independiente para ser activados, sino que ingresan e infectan las PC's con la simple visualización del mail.

1.1.3.7 Virus de arquitectura cliente / servidor

La funcionalidad de estos virus consiste en hacer que la víctima del ataque ejecute un programa que corresponde al servidor del virus, lo que conduce a su auto instalación en el sistema a la espera de que el usuario conecte su computadora a Internet. En este grupo se incluyen de manera especial a los troyanos, que más que virus, son verdaderas aplicaciones cliente / servidor, por las cuales cualquier persona, y con la configuración adecuada, puede controlar los recursos de una PC a distancia y a través de una conexión a Internet.

1.1.3.8 Troyanos

Es un programa potencialmente peligroso que se oculta dentro de otro para evitar ser detectado, e instalarse de forma permanente en el sistema. Este tipo de software no suele realizar acciones destructivas por sí mismo, pero entre muchas otras funciones, tienen la capacidad de capturar datos, generalmente contraseñas e información privada, enviándolos a otro sitio. Otra de sus funciones es dejar indefenso el sistema, abriendo brechas en la seguridad, de esta forma se puede tomar el control total de forma remota, como si realmente se estuviera trabajando delante de la pantalla. Estos programas son llamados espías, pues recolectan información del usuario con fines que pueden ser maliciosos. Algunos programas antivirus los detectan como virus o como caballos de Troya (o simplemente troyanos).

1.1.3.9 Spam (correo basura) y Spyware (software espía)

Cuando se navega en Internet, se puede encontrar ventanas que sugieren instalar ciertos programas, o que ofrecen premios y regalos. Si se acepta, se expone a que se instalen en el equipo aplicaciones de tipo spyware, adware o dialers. Los daños o inconveniencias que pueden causar son los siguientes:

- Ocupan el ancho de banda en la conexión al Internet, haciendo la navegación más lenta.
- Obligan al usuario a visitar sitios indeseados, que pueden incluir juegos de azar, productos basura y hasta contenidos indecentes.
- La lenta conexión al Internet implica que el usuario pague más dinero por el servicio de conexión.
- Usuarios maliciosos pueden estar recibiendo información privada, que incluye números de tarjetas de crédito y contraseñas.
- Un virus se puede distribuir a todos sus contactos de correo electrónico.
- En resumen, cualquier persona puede estar espiando a otra que esté navegando en Internet.

1.1.4 ANTIVIRUS

Los antivirus permiten la detección y eliminación de virus. Un virus es identificado mediante una cadena característica extraída de su código, cadena que se almacena en una base de datos. El antivirus inspecciona los ficheros en busca de cadenas asociadas a virus lo que, unido a otros síntomas propios de la modalidad de virus de que se trate, permite su identificación. Si el antivirus tiene capacidad para ello, "desinfectará" el computador.

1.2 TIPOS DE ATAQUE

1.2.1 EAVESDROPPING Y SNIFFING[7]

Muchas redes son vulnerables al eavesdropping[8], o la pasiva intercepción (sin modificación) del tráfico de red. El sniffing consiste en filtrar todos los paquetes que pasan por una red abriendo cada uno de ellos para mirar el interior, en busca de contraseñas o información útil. El sniffer puede ser colocado tanto en una estación de trabajo conectada a red, como a un equipo router o a un gateway de Internet, y esto puede ser realizado por un usuario con legítimo acceso, o por un intruso que ha ingresado por otras vías.

1.2.2 SNOOPING Y DOWNLOADING

Los ataques de esta categoría tienen el mismo objetivo que el sniffing, obtener la información sin modificarla. Sin embargo los métodos son diferentes. Además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de e-mail y otra información guardada, realizando en la mayoría de los casos una descarga de esa información a su propia computadora. El Snooping puede ser realizado por simple curiosidad, pero también es realizado con fines de espionaje y robo de información o software.

1.2.3 TAMPERING O DIDDLING

Esta categoría se refiere a la modificación desautorizada a los datos, o al software instalado en un sistema, incluyendo borrado de archivos. Este tipo de ataques son particularmente serios cuando el que lo realiza ha obtenido derechos de administrador o supervisor, con la capacidad de disparar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema.

---

[7] http://www.dric.com.mx/seguridad/di/di4.php?cat=7

[8] Eavesdropping: La interceptación o *eavesdropping*, también conocida por *passive wiretapping* es un proceso mediante el cual un agente capta información - en claro o cifrada - que no le iba dirigida; esta captación puede realizarse por muchísimos medios.

1.2.4 SPOOFING

Su objetivo es conseguir el nombre y contraseña de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él, como puede ser el envío de falsos e-mails. Los protocolos de red también son vulnerables al spoofing. Con el IP spoofing, el atacante genera paquetes de Internet con una dirección de red falsa en el campo From, pero que es aceptada por el destinatario del paquete.

1.2.5 JAMMING O FLOODING

Este tipo de ataques desactivan o saturan los recursos del sistema. Una acción común es la de enviar millares de e-mails sin sentido a todos los usuarios posibles en forma continua, saturando los distintos servidores de destino.

1.2.6 BARRIDO DE PUERTOS

Un barrido de puertos trata de identificar qué puertos TCP y UDP están abiertos en un computador para poder aprovechar ciertos servicios que dependen de ellos para entrar en el sistema.

1.2.7 DETECCIÓN DE PROXIES

El atacante desea encontrar proxies mal configurados o de mala calidad para convertir sus ataques en anónimos. Dado que casi todos los servidores llevan un registro de las direcciones IP desde las que se accede a ellos, si un intruso quisiera atacarlos sería fácil seguirle la pista a través de su IP.

1.2.8 ATAQUES SMURF/FRAGGLE[9]

Es una técnica de ataque masivo a servidores basada en el envío de paquetes de difusión a los computadores de una subred. Estos paquetes llevan una falsa dirección de origen, apuntando en realidad a un servidor que se desea atacar

[9] http://www.kernelnet.com/content/view/172/2/

(técnica conocida como spoofing). La diferencia entre el ataque Smurf y el ataque Fraggle consiste en el tipo de paquete enviado.

1.2.9 LAND

Este ataque se basa en poner la misma dirección (vía IP spoofing) de origen y destino. Muchos equipos al ver un paquete de esas características, entran en un ciclo infinito (loop) hasta que se cae el sistema.

1.2.10 TEARDROP

Se basa en el envío de un mensaje TCP en diversos paquetes que se traslapan. Algunos sistemas operativos tienen problemas para reensamblar paquetes traslapados, ocasionando caídas.

1.3 MÉTODOS DE HACKING[10]

1.3.1 CABALLOS DE TROYA

Consiste en introducir dentro de un programa una rutina o conjunto de instrucciones, por supuesto no autorizadas y que la persona que lo ejecuta no conoce, para que dicho programa actúe de una forma diferente a como estaba previsto.

1.3.2 SUPERZAPPING

Se denomina superzapping al uso no autorizado de un programa editor de ficheros para alterar, borrar, copiar, insertar o utilizar en cualquier forma no permitida los datos almacenados en los soportes de un computador. El nombre proviene de una utilidad llamada SUPERZAP diseñada para Mainframes y que permite acceder a cualquier parte del computador y modificarlo.

1.3.3 PUERTAS FALSAS

Es una práctica acostumbrada en el desarrollo de aplicaciones complejas que los programadores introduzcan interrupciones en la lógica de los programas para chequear la ejecución, producir salidas de control, etc. Con el objeto de producir un atajo para ir corrigiendo los posibles errores. Lo que ocurre es que en la mayoría de los casos cuando el programa se entrega al usuario estas rutinas no se eliminan del programa y proveen al hacker de accesos o facilidades en su labor si sabe descubrirlas.

1.3.4 BOMBAS LÓGICAS

Consiste en introducir un programa o rutina que en una fecha determinada destruirá o modificará la información, o provocará la caída del sistema.

---

[10] http://www.geocities.com/delincuentes_digitales/anteced.htm

1.4 VULNERABILIDADES DE LOS SISTEMAS OPERATIVOS

La mayoría de los ataques se basan en fallos de diseño inherentes a Internet (y sus protocolos) y a los sistemas operativos utilizados, por lo que no son "solucionables" en un corto plazo.

La solución inmediata en cada caso es mantenerse informado sobre todos los tipos de ataques existentes y las actualizaciones que permanentemente lanzan las empresas desarrolladoras de software, principalmente de sistemas operativos.

Muchos sistemas están expuestos a "agujeros" de seguridad que son explotados para acceder a archivos, obtener privilegios o realizar sabotaje. Estas vulnerabilidades ocurren por varias razones, y miles de "puertas invisibles" son descubiertas (cada día) en sistemas operativos, aplicaciones de software, protocolos de red, exploradores de Internet, correo electrónico y toda clase de servicios informáticos disponibles.

Los Sistemas operativos abiertos (como Unix y Linux) tienen agujeros más conocidos y controlados que aquellos que existen en sistemas operativos cerrados (como Windows). La importancia (y ventaja) del código abierto radica en miles de usuarios que analizan dicho código en busca de posibles bugs y ayudan a obtener soluciones en forma inmediata.

Actualmente, se están descubriendo casi de forma continua, vulnerabilidades en los sistemas operativos Windows de Microsoft. Por esta razón, se editan parches para corregir las deficiencias del sistema Windows frente a posibles ataques maliciosos.

1.5 VULNERABILIDADES DE LOS PROTOCOLOS DE COMUNICACIÓN[11]

Los protocolos son como reglas de comunicación que permiten el flujo de información entre computadoras distintas que manejan lenguajes distintos, por ejemplo, dos computadores conectados en la misma red pero con protocolos diferentes no podrían comunicarse jamás, para ello, es necesario que ambas "hablen" el mismo idioma, por tal sentido, el protocolo TCP/IP fue creado para las comunicaciones en Internet. Para que cualquier computador se conecte a Internet, es necesario que tenga instalado este protocolo de comunicación.

Los principales protocolos de comunicación se detallan a continuación:

1.5.1 TCP/IP

El protocolo TCP/IP (Transmition Control Protocol/Internet Protocol) hace posible enlazar cualquier tipo de computadoras, sin importar el sistema operativo que usen o el fabricante. Este sistema de IP permite a las redes enviar correo electrónico (e-mail), transferencia de archivos (FTP) y tener una interacción con otras computadoras (TELNET) no importando donde estén localizadas, tan solo que sean accesibles a través de Internet.

Los protocolos que se utilizan en las comunicaciones son una serie de normas que deben aportar las siguientes funcionalidades:

- Permitir localizar un computador de forma inequívoca.
- Permitir realizar una conexión con otro computador.
- Permitir intercambiar información entre computadores de forma segura, independiente del tipo de maquinas que estén conectadas.
- Permitir liberar la conexión de forma ordenada.

[11] http://www.vsantivirus.com/ev-vul-tcp.htm

Los protocolos de comunicación definen las normas que posibilitan que se establezca una comunicación entre varios equipos o dispositivos, ya que estos equipos pueden ser diferentes entre sí. Una interfaz, sin embargo, es el encargado de la conexión física entre los equipos, definiendo las normas para las características eléctricas y mecánicas de la conexión.

1.5.1.1 Vulnerabilidades en el protocolo TCP

La que sería una importante vulnerabilidad en el protocolo TCP, consiste en que cualquier atacante podría interrumpir a su antojo todas las conexiones realizadas entre servidores y routers, causando un gran caos en Internet.

Junto a IP, TCP es uno de los protocolos fundamentales para el funcionamiento de Internet. Y aunque aún existe cierta confusión sobre los detalles del problema, la mayoría de los escenarios afectados son tremendamente críticos. En principio serían todos aquellos que utilizan conexiones de larga duración y gran ancho de banda.

Uno de los protocolos más afectados por esta vulnerabilidad en TCP, es el llamado BGP (Border Gateway Protocol), que se emplea para el intercambio de información de enrutamiento y el mantenimiento de las tablas de direcciones IP, y que hace uso intensivo de las conexiones TCP, sin utilizar ningún tipo de autenticación. Además del protocolo BGP, otros protocolos como DNS (usado para la resolución de nombres), y todos los protocolos que utilizan cifrado SSL, también serían vulnerables.

Casi cualquier protocolo que se basa en la utilización de conexiones TCP persistentes en el tiempo, y cuyos puertos y direcciones IP puedan ser identificados (prácticamente todos los servicios de Internet conocidos), serían vulnerables.

Por lo general cualquier protocolo que se base en la utilización de conexiones TCP persistentes (larga duración), que utilicen un puerto TCP de

origen fácilmente identificable y con direcciones IP del origen y el destino identificables pueden llegar a ser vulnerables.

1.5.1.2 Vulnerabilidad de Kerberos

Kerberos es el protocolo predefinido que proporciona la autenticación segura de usuario en Windows, siendo además un estándar de la industria. Existe una vulnerabilidad capaz de provocar una denegación de servicio en este protocolo.

Esto permite que un atacante pueda enviar un mensaje especialmente modificado a un controlador de dominio, causando que el servicio responsable de la autenticación de usuarios en un Directorio Activo de dominio, deje de responder.

Se ha detectado un problema de seguridad que podría permitir a un usuario malintencionado obtener acceso a información confidencial transmitida a través de un equipo basado en Microsoft Windows dentro de un entorno de dominio y realizar ataques por denegación de servicio contra los controladores del dominio. Puede mejorar la protección del equipo con esta actualización de Microsoft. Tras instalar este elemento, es posible que deba reiniciar el equipo.

1.5.1.3 Vulnerabilidad de PKINIT

PKINIT es el protocolo utilizado por el proceso de autenticación basado en claves públicas integrado con el sistema de control de acceso Kerberos de Windows. Existe una vulnerabilidad en este protocolo que puede permitir la revelación de información y el spoofing (falsificación) de servidor.

Un atacante puede interferir con cierta información que se envía a un controlador de dominio y potencialmente acceder a comunicación sensible de la red del cliente. Los usuarios pueden creer estar accediendo a un servidor confiable, cuando en realidad están en un servidor malicioso controlado por el atacante. Para que el ataque sea exitoso, el atacante debe inyectarse primero en el medio de una sesión de autenticación como intermediario entre el cliente y el controlador de dominio.

CAPITULO II

SEGURIDAD EN REDES

2.1 SEGURIDAD EN REDES

2.1.1 INTRODUCCIÓN

El objetivo de la seguridad en redes es describir cuales son los métodos más comunes que se utilizan para incidir ataques a la seguridad informática de una organización, y qué armas se puedan implementar para la defensa, ya que es importante saber cómo pueden atacar y qué soluciones se tienen para prevenir, detectar y reparar un siniestro de este tipo. Los ataques pueden servir a varios objetivos incluyendo fraude, extorsión, robo de información, o simplemente el desafío de penetrar un sistema. Esto puede ser realizado por empleados internos de la organización que abusan de sus permisos de acceso, o por atacantes externos que acceden remotamente o interceptan el tráfico de red.

2.1.2 DEFINICIÓN

Seguridad en redes es mantener bajo protección los recursos y la información con que se cuenta en la red, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo actuado.

En la seguridad de un sistema informático, hay tres conceptos que entran en discusión: vulnerabilidad o inseguridad, amenazas y contramedidas.

2.1.3 VULNERABILIDAD

Punto o aspecto del sistema que es susceptible de ser atacado o de dañar la seguridad del mismo. Representan las debilidades o aspectos falibles o atacables en el sistema informático.

2.1.4 AMENAZA

Posible peligro del sistema. Puede ser una persona (hacker) o un programa (virus, caballo de Troya). Representan los posibles atacantes o factores que aprovechan las debilidades del sistema.

2.1.5 CONTRAMEDIDA

Técnicas de protección del sistema contra las amenazas. La seguridad informática se encarga de la identificación de las vulnerabilidades del sistema y del establecimiento de contramedidas que eviten que las distintas amenazas posibles exploten dichas vulnerabilidades. Una máxima de la seguridad informática es que: "No existe ningún sistema completamente seguro". Existen sistemas más o menos seguros, y más o menos vulnerables, pero la seguridad nunca es absoluta.

No se puede hablar de un sistema informático totalmente seguro, sino más bien de uno en el que no se conocen tipos de ataques que puedan vulnerarlo, debido a que se han establecido medidas contra ellos.

2.1.6 CATEGORIZACIÓN DE LAS AMENAZAS A LA SEGURIDAD EN REDES

Las amenazas a la seguridad en redes se pueden clasificar en cuatro categorías:

2.1.6.1 Amenazas no estructuradas

Suelen ser originadas por personas inexpertas que utilizan herramientas de piratería e Internet. Algunas de estas personas suelen obrar de mala fe, pero la mayoría se ve arrastrada por los retos intelectuales que suelen conocerse como script kiddies. Suponen una amenaza a la seguridad de las redes. Ya que pueden introducir un virus en la red, sin ser concientes de las consecuencias que pueden provocar.

2.1.6.2 Amenazas estructuradas

Son causadas por personas mucho más competentes a nivel técnico que los script kiddies, ya que conocen los diseños de los sistemas y sus puntos débiles. Pueden entender y crear scripts piratas que penetren en el sistema y además suelen dirigirse a un destino o grupo específico.

2.1.6.3 Amenazas externas

Suelen ser causadas por personas ajenas a la propia empresa, pero que no tienen acceso autorizado a los sistemas o a la red de la empresa. Por lo general entran en una red desde Internet o desde servidores de acceso telefónico.

2.1.6.4 Amenazas internas

Normalmente, son causadas por personas que tienen acceso autorizado a la red. Según las estadísticas, la mayoría de incidentes de seguridad proviene de este tipo de amenazas.

2.1.7 MÉTODOS DE SEGURIDAD

Para tener una buena seguridad hay que tener en cuenta tres factores: la prevención, la recuperación y la detección.

2.1.7.1 Prevención

La prevención se encarga de preparar el equipo para recibir los ataques, mantener una buena política de seguridad y poder reaccionar al momento, para así evitar el ataque. Un ejemplo de prevención son los firewalls ya que ayudan a evitar el ataque. Dentro de prevención se encuentra también todo lo que se refiere a hacer unas buenas copias de seguridad, mantener diferentes equipos encargándose de la seguridad a la vez, etc.

2.1.7.2 Detección

La detección se encarga de descubrir los ataques en el momento que se están realizando, y así poder contrarrestarlos debidamente. Un ejemplo de detección seria un IDS bien configurado, que sepa al momento lo que esta ocurriendo y nos avise debidamente.

2.1.7.3 Recuperación

Consiste en recuperar todo el equipo como se encontraba en un principio borrando el ataque para poder continuar normalmente. Dentro de la recuperación se puede encontrar también la localización del atacante.

2.1.8 CONSEJOS DE SEGURIDAD

- Dar acceso al sistema sólo a los usuarios que vayan a hacer uso del equipo, y otorgarles los mínimos privilegios necesarios, vigilando después desde dónde se conectan para controlar posibles intrusiones si aparecen lugares sospechosos.
- Mantener al día las cuentas del sistema, minimizando el fichero de *passwd* con la eliminación de algunas cuentas creadas por defecto como games, daemon, nobody.
- Verificar los atributos *setsuid* de los ficheros propiedad del root.
- Habilitar sólo aquellos puertos y servicios que se van a usar: Ftp, Telnet, Mail y configurarlos de manera correcta.
- Hacer uso de NIS (*Network Information Services*, que permite la compartición de ficheros de passwd, hosts...) y NFS, sólo cuando sea imprescindible, dados los problemas de configuración que suponen.
- Vigilar los registros (*logs*) que guarda el sistema operativo, especialmente los generados por syslogd y klogd, que monitorizan las acciones que se llevan dentro del sistema, ya que pueden ayudar a encontrar posibles intrusos. Además se puede hacer uso de *Tripewire*, una herramienta más, que inspecciona los cambios en ficheros clave del sistema.

- Disponer de las últimas versiones de servidores Web, así como de sistemas operativos en constante evolución y actualizados, como Linux.
- Conservar las listas de correo que informan de los problemas detectados en programas y sistemas operativos, así como de los parches a esos *bugs*.
- La aplicación inadecuada de los parches para las vulnerabilidades de software pueden causar inoperabilidad del sistema, crear debilidades en la seguridad y alterar los componentes críticos del sistema o la información. Además pueden dejar desprotegidos los sistemas informáticos y exponerlos al uso indebido por parte de personas no autorizadas, como los hackers informáticos. Siguiendo consistentemente los procedimientos de administración de parches, se podrá reducir los riesgos asociados a las vulnerabilidades de software.
- Es recomendable aplicar una buena contraseña que tenga por lo menos ocho caracteres que incluyan tanto letras como números. Una política que pida a los usuarios que cambien sus contraseñas con frecuencia, también reduce el riesgo de una violación a los sistemas.

2.2 MECANISMOS DE SEGURIDAD EN REDES[12]

Las amenazas actuales son más frecuentes y avanzadas tanto en sus métodos de propagación como en los daños que causan. La complejidad de las amenazas en cuanto al ataque y a la propagación, junto a la creciente complejidad de las redes, indican que las medidas de seguridad por sí solas ya no son adecuadas. Para esto se debe implementar medidas de seguridad en todos los puntos vulnerables del sistema, como los servidores y equipos de escritorio, y establecer una completa línea de defensa de múltiples capas o “protección total”.

Elementos indispensables en la seguridad de redes:

2.2.1 EL SOFTWARE ANTIVIRUS

Brinda protección contra los archivos que entran a la red a través del correo electrónico, descargas de Internet, disquetes, etc. El software antivirus debe buscar automáticamente las amenazas más recientes, explorar con frecuencia los sistemas en busca de estas amenazas y también vigilar en tiempo real cuando se descargan nuevos archivos de Internet o se separan de los mensajes de correo electrónico para garantizar que nada peligroso ingrese. El software antivirus no solo debe proteger las estaciones de trabajo y servidores, sino también los firewalls y aplicaciones importantes como los servidores Web y de correo electrónico para poder evitar muchos problemas.

2.2.2 LOS FIREWALLS

Son una importante línea de defensa de la red y de toda la información que entra y sale de la misma para garantizar que no sucedan accesos no autorizados. Los firewalls también ayudan a proteger un computador de los ataques de DOS.

---

[12] http://www.symantec.com/region/mx/smallbusiness/articles/LAM_depth.html

2.2.3 EL SOFTWARE DE DETECCIÓN DE INTRUSOS O IDS

Monitorea constantemente la red en busca de actividades sospechosas o ataques directos para que se pueda actuar inmediatamente. La detección de intrusos es especialmente útil cuando se utiliza conjuntamente con un firewall.

2.2.4 LAS REDES PRIVADAS VIRTUALES (VPN)

Protegen las conexiones remotas más allá del perímetro para poder establecer comunicaciones seguras en Internet.

2.2.5 CONFIGURACIÓN DEL DISCO

Permite hacer copias de seguridad de la información y recuperarla en su estado inicial seguro y poder confiar en la integridad de la información.

2.2.6 OTRAS MEDIDAS QUE SE PUEDEN TOMAR

Además de la tecnología para la seguridad, se puede tomar otras medidas para reforzar la protección total de la información:

- **Actualizar parches:** se debe actualizar los sistemas operativos, aplicaciones y productos de seguridad con los últimos parches para sellar muchas puertas abiertas que las amenazas han usado para difundirse.
- **Crear una política de seguridad:** Establecer cuáles son los recursos valiosos de información y los derechos de acceso a la misma. También se deben determinar normas para el acceso remoto.
- **Entrenamiento para tomar consciencia sobre la seguridad:** Instruir a los usuarios para que conozcan sus funciones en relación con el mantenimiento de la seguridad de la información.
- **Restringir y controlar el acceso a la red:** es importante asignar únicamente los permisos que el usuario necesita para acceder a la red.
- **Reforzar la administración de contraseñas:** es elemental que los usuarios cambien con frecuencia sus contraseñas y tengan cuidado de no anunciarlas públicamente.

2.3 VIOLACIONES A LA SEGURIDAD EN LAS REDES

Existen tres tipos de ataques a una red:

2.3.1 Ataques de reconocimiento

Un intruso trata de descubrir sistemas, servicios y puntos débiles.

El reconocimiento tiene lugar cuando un usuario no autorizado trata de descubrir dispositivos, servicios disponibles y puntos débiles del sistema de red. También se conoce como recopilación de información y suele preceder a un acceso real o a un ataque de denegación de servicio.

El intruso primero barre la red con pings para determinar que direcciones IP están activas y responden. Esto permite localizar información acerca de los servicios o puertos activos en las direcciones IP. Con esta información, el intruso consulta los puertos de la aplicación con el fin de determinar el tipo y versión de la aplicación y del sistema operativo que se está ejecutando en el host de destino.

2.3.2 Ataques de acceso

Un intruso ataca las redes o sistemas para recuperar datos, obtener acceso o incrementar sus privilegios de acceso personales.

El acceso es un término muy amplio que hace referencia a la capacidad que tiene un origen completo de conectarse con un destino concreto. Luego de determinar el destino, el atacante usa algún software para llegar a él. Un ataque de acceso puede materializarse como recuperación y manipulación no autorizada de datos, un acceso al sistema o incremento de privilegios. Además pueden ser utilizados para obtener el control de un sistema e instalar y ocultar software para que los hackers lo utilicen posteriormente.

2.3.3 Recuperación no autorizada de datos

Consiste en leer, escribir, copiar o trasladar archivos a los cuales el intruso no puede acceder. El intruso solo tendrá problemas cuando el archivo esté cifrado y no pueda ser leido.

2.3.4 Acceso no autorizado al sistema

La obtención de acceso a sistemas que incorporen cierta seguridad puede implicar la ejecución de un script o el uso de una herramienta que explote un punto débil de la aplicación o sistema que está siendo atacado. Los puntos débiles del sistema operativo también pueden ser utilizados para proporcionar un acceso no autorizado al sistema.

2.3.5 Incremento no autorizado de los privilegios

Los usuarios legítimos con niveles muy bajos de privilegio o los intrusos que tienen un acceso muy restringido son los más propensos a realizar este tipo de ataque. El objetivo es obtener información o procedimientos de ejecución para los que no tiene acceso autorizado. Esto implica obtener acceso raíz a un sistema Unix e instalar un sniffer para capturar el tráfico de la red. El objetivo final consiste en localizar nombres de usuario y contraseñas que puedan ser utilizados para acceder a otro destino.

2.3.6 Ataques de Denegación de Servicio (DoS)

Tiene lugar cuando un atacante desactiva o corrompe las redes, los sistemas o los servicios para denegar el servicio a los usuarios. Esto implica que el sistema se colapse o que se ralentice hasta un punto que sea inutilizable. Estos ataques también pueden ser tan sencillos como borrar o corromper información necesaria. Generalmente, el ataque consiste en ejecutar un script o una herramienta. El atacante no necesita tener acceso previo al destino, sino solo una ruta a éste.

Un ataque de denegación de servicio distribuida (DDoS) es aquel en el que el origen del ataque proviene de muchas computadoras, haciendo que sea muy complicado localizar y detener el origen.

2.4 FIREWALLS

2.4.1 INTRODUCCIÓN

Un firewall en Internet es un sistema o grupo de sistemas que imponen una política de seguridad entre la red privada de la organización e Internet. Para lograr la efectividad de un firewall, todo el tráfico de información de Internet deberá pasar a través del mismo. Así, toda la información será inspeccionada mediante el uso de políticas de seguridad y monitoreos de los registro de seguridad. De esta manera se crea un perímetro de defensa, diseñado para proteger la información.

Los Firewall son filtros que bloquean o permiten conexiones y transmisiones de información por Internet. Los filtros están diseñados para evitar que un usuario irreconocible ataque al equipo vía Internet.

Es importante aclarar que un firewall de Internet no es justamente un ruteador, un servidor de defensa, o una combinación de elementos que proveen seguridad para la red. El firewall es parte de una política de seguridad completa que crea un perímetro de defensa diseñada para proteger las fuentes de información. Esta política de seguridad podrá incluir publicaciones con las guías de ayuda donde se informe a los usuarios de sus responsabilidades, normas de acceso a la red, política de servicios en la red, política de autenticidad en acceso remoto o local a usuarios propios de la red, normas de dial-in y dial-out, reglas de encriptación de datos y discos, normas de protección de virus, y entrenamiento. Todos los puntos potenciales de ataque en la red podrán ser protegidos con el mismo nivel de seguridad.

El firewall analiza los datos procedentes de Internet, eliminando el tráfico no deseado. Típicamente sólo permiten el tráfico de páginas web, cortando todos los demás servicios (Chat, transferencia de ficheros ftp, telnet, control remoto, etc). De esta forma protegen a los computadores frente a las posibles amenazas procedentes de Internet. Estos ataques pueden ocasionar el bloqueo del computador, la infección por un virus informático y el robo de datos o ficheros.

Algunas aplicaciones pueden requerir que se abran ciertos puertos o conexiones del firewall. En estos casos conviene que los cambios introducidos sean lo más restrictivos que sea posible.

Para el correcto funcionamiento de un firewall es necesario mantenerlo actualizado. Constantemente se descubren nuevas vulnerabilidades y se actualizan los programas de seguridad.

2.4.2 FUNCIONAMIENTO DE UN FIREWALL

Para poner a funcionar un sistema firewall es necesario tomar en cuenta cinco aspectos importantes:

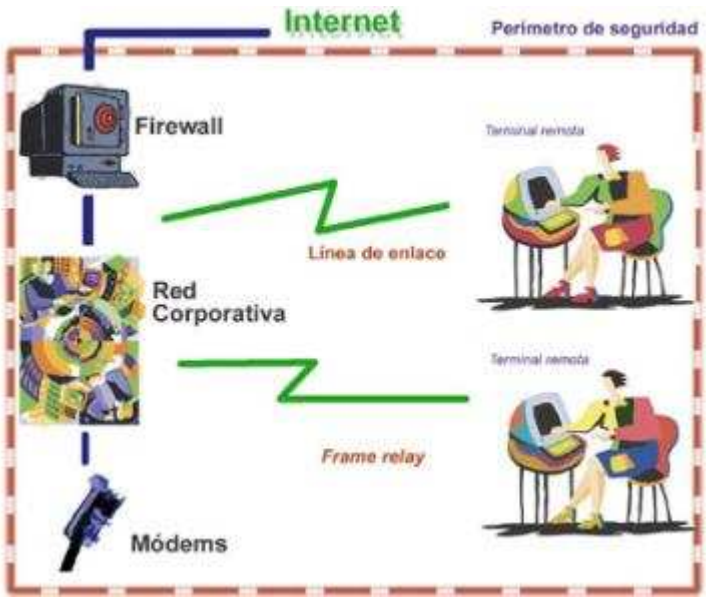


Figura 1.- Funcionamiento de un Firewall[13]

Un Firewall se conecta entre la red interna confiable y la red externa no confiable (Figura 1). Los Firewalls en Internet administran los accesos posibles de la Internet a la red privada. Si no se cuenta con este sistema, cada uno de los servidores de la red se exponen al ataque de otros servidores.

[13] http://redescolar.ilce.edu.mx/redescolar/Revista/10/articulos/08.html

El sistema opera en las capas superiores del modelo OSI y tiene información sobre las funciones de la aplicación en la que basan sus decisiones. También opera en las capas de red y transporte, en cuyo caso, examina los encabezados IP y TCP (paquetes entrantes y salientes), y rechaza o acepta paquetes con base en reglas de filtración de paquetes programadas.

Así, el Firewall actúa como el punto de cierre que monitorea y rechaza el tráfico en la red en el nivel de la aplicación (Figura 2).

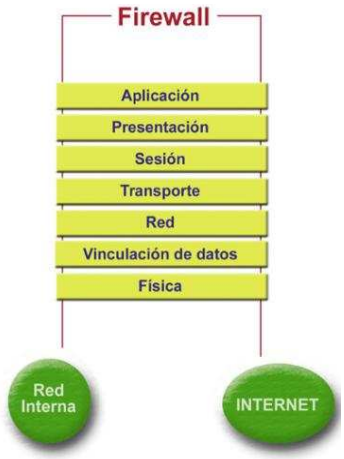


Figura 2.- Firewall a nivel de capas[14]

Un firewall es una herramienta de seguridad que se encarga de aislar redes o sistemas informáticos respecto de otros que se encuentran en la misma red. Constituye una especie de “barrera lógica” delante de los sistemas que examina todos y cada uno de los paquetes de información que tratan de atravesarla. En función de unos criterios establecidos previamente deciden qué paquetes deben pasar y cuáles deben ser bloqueados. Muchos son capaces de filtrar el tráfico de datos que intenta salir de la red al exterior, evitando así que los troyanos sean efectivos.

[14] http://redescolar.ilce.edu.mx/redescolar/Revista/10/articulos/08.html

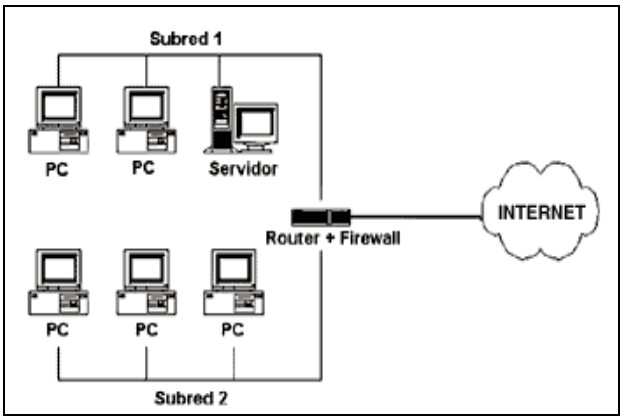


Figura 3.- Un firewall se coloca "en medio" de las comunicaciones entre un computador (o red local) e Internet, filtrando todo el tráfico que lo atraviesa y tomando decisiones de qué hacer con él en función de reglas establecidas

Todas las comunicaciones de Internet se realizan mediante el intercambio de paquetes de información, que son la unidad mínima de datos transmitida por la red. Para que cada paquete pueda llegar a su destino, independientemente de donde se encuentren las máquinas que se comunican, debe llevar anexa la información referente a la dirección IP de cada máquina en comunicación, así como el puerto a través del que se comunican. La dirección IP de un dispositivo lo identifica de manera única dentro de una red.

Un firewall intercepta todos y cada uno de los paquetes destinados o provenientes de un computador, y lo hace antes de que ningún otro servicio los pueda recibir. Es decir el firewall puede controlar de manera exhaustiva todas las comunicaciones de un sistema a través de Internet.

2.4.2.1 Los componentes del sistema [15]

Un Firewall típico se compone de una combinación de: ruteador filtra-paquetes, gateway a nivel aplicación y gateway a nivel-circuito.

Las funciones de cada componente son las siguientes: el ruteador toma las decisiones de cerrar y permitir el paso de cada uno de los paquetes que son recibidos. Éste sistema se basa en el examen de cada datagrama enviado y

[15] http://redescolar.ilce.edu.mx/redescolar/Revista/10/articulos/08.html

cuenta con una regla de revisión de información de los encabezados IP; si éstos no corresponden a las reglas, se descarta o desplaza el paquete (Figura 4).

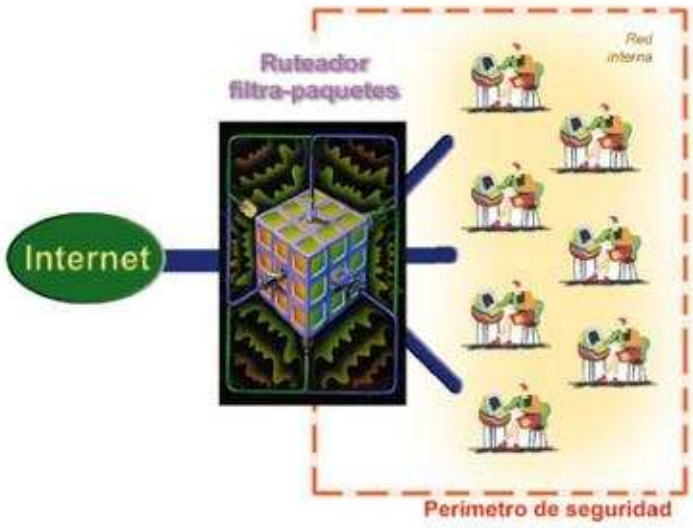


Figura 4.- Ruteador Filtra Paquetes[16]

Por su parte, los gateways del nivel de aplicación permiten al administrador de red la implementación de una política de seguridad más estricta que la que permite un ruteador filtra-paquetes. Esto es mucho mejor que depender de una herramienta genérica de filtra-paquetes para administrar la circulación de los servicios de Internet a través del Firewall. Se puede instalar en el gateway un código de propósito-especial (un servicio Proxy) para cada aplicación deseada.

Finalmente, un gateway a nivel-circuito es, en sí, una función que puede s perfeccionada en un gateway a nivel-aplicación. "A nivel-circuito" simplemente significa que trasmite las conexiones TCP sin cumplir cualquier proceso adicional de filtrado de paquetes. La figura 5 muestra la operación de una conexión típica Telnet a través de un gateway a nivel-circuito.

Este gateway simplemente trasmite la conexión a través del Firewall sin examinarlo adicionalmente, filtrarlo, o dirigiendo el protocolo de Telnet. El gateway

[16] http://redescolar.ilce.edu.mx/redescolar/Revista/10/articulos/08.html

a nivel-circuito acciona como un cable copiando los bytes antes y después entre la conexión interna y la conexión externa.

2.4.2.2 Características y ventajas [17]

a) ***Protección de la Red.*** Mantiene alejados a los piratas informáticos (crakers) de la red al mismo tiempo que permite el acceso a todos los usuarios de la misma.

b) ***Control de acceso a los recursos de la red.*** Al encargarse de filtrar, en un primer nivel, antes que lleguen los paquetes al resto de las computadoras de la red, el Firewall es idóneo para implementar en él los controles de acceso.

c) ***Control de uso de Internet.*** Permite bloquear el material no adecuado, determinar qué sitios puede visitar el usuario de la red interna y llevar un registro.

d) ***Concentra la seguridad.*** Facilita la labor a los responsables de seguridad, dado que su máxima preocupación es encarar los ataques externos y vigilar manteniendo un monitoreo.

e) ***Control y estadísticas.*** Permite controlar el uso de Internet en el ámbito interno, conocer los intentos de conexiones desde el exterior y detectar actividades sospechosas.

f) ***Choke-Point.*** Permite al administrador de la red definir un embudo manteniendo al margen los usuarios no-autorizados y prohibiendo potencialmente la entrada o salida.

---

[17] http://redescolar.ilce.edu.mx/redescolar/Revista/10/articulos/08.html

g) ***Genera Alarmas de Seguridad.*** El administrador del Firewall puede responder una alarma y examina regularmente los registros de base.

h) ***Audita y registra Internet.*** Permite al administrador de red justificar el gasto que implica la conexión a Internet, localizando con precisión los cuellos de botella potenciales del ancho de banda.

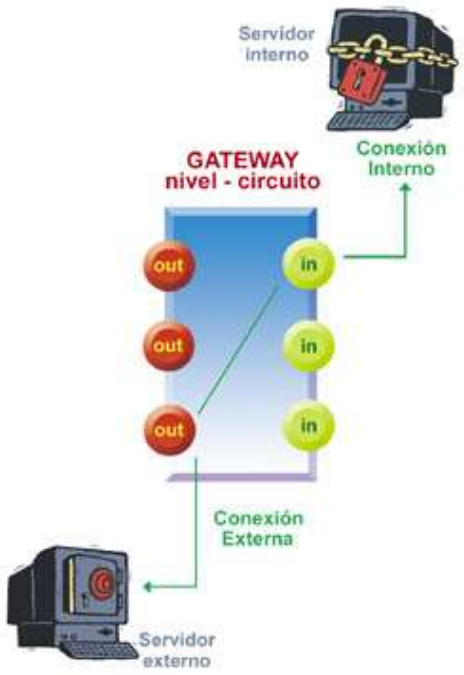


Figura 5.- Gateway a nivel circuito[18]

2.4.2.3 Ventajas

Se puede resumir las ventajas de instalar un firewall en los siguientes puntos, que son los más importantes:

- Proteger el computador de los ataques que se produzcan desde máquinas situadas en Internet.
- Asegurar que un computador no se utiliza para atacar a otros.

[18] http://redescolar.ilce.edu.mx/redescolar/Revista/10/articulos/08.html

- Prevenir el uso de troyanos que puedan existir en el sistema debido a que se hayan introducido a través de correo electrónico o en algún dispositivo de almacenamiento.
- Detectar patrones de ataques e identificar de dónde provienen.
- Evitar que un computador pueda ser un punto de entrada a una red privada virtual en el caso de utilizarlo para acceso remoto.

2.4.2.4 Diseño de decisión de un Firewall de Internet

Al diseñar un Firewall de Internet se deben tomar algunas consideraciones:

2.4.2.4.1 Políticas que propone el Firewall

"No todo lo específicamente permitido está prohibido" y "No todo lo específicamente prohibido está permitido". La primera clave, asume que un Firewall puede obstruir todo el tráfico y cada uno de los servicios o aplicaciones deseadas. La segunda, indica que el Firewall puede desplazar todo el tráfico y que cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso. Con esto, la política de seguridad se basará en una conducción cuidadosa, analizando la seguridad y la asesoría en caso de riesgo.

2.4.2.4.2 El costo financiero del proyecto Firewall

Es el precio que puede ofrecer una organización por su seguridad, un paquete filtrado puede tener un costo mínimo, ya que la organización sólo necesita un ruteador conectado al Internet, y dicho paquete ya está incluido en el equipo.

2.4.2.5 Limitaciones [19]

Un Firewall no puede proteger contra aquellos ataques que se efectúen fuera de su punto de operación, en este caso: conexión dial-out sin restricciones que

[19] http://www.monografias.com/trabajos3/firewalls/firewalls.shtml

permita entrar a una red protegida. El usuario puede hacer una conexión SLIP o PPP a Internet. Este tipo de conexiones derivan de la seguridad provista por un Firewall construido cuidadosamente, creando una puerta de ataque.

El Firewall no puede proteger de las amenazas a las que lo sometan usuarios inconscientes. Además no puede prohibir que espías corporativos copien datos sensitivos en dispositivos de almacenamiento.

No puede proteger contra los ataques de la ingeniería social, en este caso, un hacker que quiera ser un supervisor o aquel que persuade a los usuarios menos sofisticados.

No puede proteger de los ataques posibles a la red interna por virus informativos llegados a través de archivos y software.

Tampoco puede proteger contra los ataques en la transferencia de datos. Éstos ocurren cuando datos aparentemente inocuos son enviados o copiados a un servidor interno y ejecutados, abriendo la puerta al ataque.

2.4.2.6 Beneficios de un Firewall en Internet[20]

Los firewalls en Internet administran los accesos posibles del Internet a la red privada. Sin un firewall, cada uno de los servidores propios del sistema se expone al ataque de otros servidores en el Internet. Esto significa que la seguridad en la red privada depende de la “Dureza” con que cada uno de los servidores cuenta y es únicamente seguro tanto como la seguridad en la fragilidad posible del sistema.

El firewall permite al administrador de la red definir un "choke point" (embudo), manteniendo al margen los usuarios no-autorizados (tal como: hackers, crakers y espías) fuera de la red, prohibiendo potencialmente la entrada o salida al vulnerar

[20] http://www.monografias.com/trabajos3/firewalls/firewalls.shtml

los servicios de la red, y proporcionar la protección para varios tipos de ataques posibles. Uno de los beneficios clave de un firewall en Internet es que ayuda a simplificar los trabajos de administración, una vez que se consolida la seguridad en el sistema firewall, es mejor que distribuirla en cada uno de los servidores que integran la red privada.

2.4.3 TIPOS DE FIREWALL[21]

Se puede identificar tres grupos, en función de los criterios de diseño y el segmento de mercado al que apuntan.

2.4.3.1 Firewalls de Hardware

Es un equipo en el que está integrado el software y hardware para operar. Debido a su gran rendimiento, son utilizados en grandes empresas, y es necesario que sean administrados por personal técnico especializado.

2.4.3.2 Firewalls de Software Corporativos

Una ventaja es la flexibilidad que tienen, ya que permiten adaptarse al software y al hardware disponible. Ya que deben convivir con el sistema operativo, son más complicados de instalar y mantener, además del hecho que necesitan personal con conocimiento del producto y el sistema operativo. Hay modelos que protegen redes enteras y otros específicos para defender servidores.

2.4.3.3 Firewalls Personales

Están diseñados para brindar la máxima seguridad posible, haciendo un balance entre el nivel de protección, facilidad de uso y mantenimiento. La mayoría tienen asistentes de configuración, así como también varias configuraciones predeterminadas que ayudan a mantener un alto nivel de seguridad sin perder

---

[21] http://www.microsoft.com/latam/seguridad/hogar/articulos/firewall.asp

funcionalidad. Muchos de ellos poseen servicios de actualización automática y suman capacidades de detección de tráfico malicioso.

2.4.3.4 Conclusiones

Mediante la imposición de políticas de seguridad, el Firewall proporcionará la mayoría de las herramientas para complementar su seguridad en la red, en el acceso a los recursos de la red y hacia la red externa. Es importante establecer que un monitoreo constante del registro base nos permitirá detectar cualquier posible intruso y proteger la información.

2.4.4 IDS (INTRUSION DETECTION SYSTEM)[22]

Un IDS o Sistema de Detección de Intrusiones es una herramienta de seguridad que intenta detectar o monitorizar los eventos ocurridos en un determinado sistema informático o red informática en busca de intentos de complicar la seguridad de dicho sistema.

Los IDS buscan patrones previamente definidos que impliquen cualquier tipo de actividad sospechosa o maliciosa sobre la red o host.

Previenen y dan alerta anticipada ante cualquier actividad sospechosa. No están diseñados para detener un ataque, aunque sí pueden generar ciertos tipos de respuesta ante éstos.

Aumentan la seguridad de un sistema, vigilan el tráfico de una red, examinan los paquetes analizándolos en busca de datos sospechosos y detectan las primeras fases de cualquier ataque como pueden ser el análisis de la red, barrido de puertos, etc.

---

[22] http://www.maestrosdelweb.com/editorial/snort/

2.4.4.1 Clasificación de los IDS

Por el tipo de respuesta podemos clasificarlos en:

2.4.4.1.1 Pasivos

Son aquellos IDS que notifican a la autoridad competente o administrador de la red mediante el sistema que sea. Pero no actúa sobre el ataque o atacante.

2.4.4.1.2 Activos

Generan algún tipo de respuesta sobre el sistema atacante o fuente de ataque como cerrar la conexión o enviar algún tipo de respuesta predefinida en la configuración.

2.4.4.2 Posición del IDS

Si se colocan los IDS antes del firewall se podrá capturar todo el tráfico de entrada y salida de la red. La posibilidad de falsas alarmas es grande.

La colocación detrás del firewall monitorizará todo el tráfico que no se ha detectado y detenido por el firewall o cortafuegos, por lo que será considerado como malicioso en un alto porcentaje de los casos. La posibilidad de falsas alarmas es muy inferior.

Algunos administradores de sistemas colocan dos IDS, uno delante y otro detrás del cortafuegos para obtener información exacta de los tipos de ataques que recibe la red ya que si el cortafuegos está bien configurado puede parar o filtrar muchos ataques.

2.4.4.3 La labor del software para la detección de intrusiones

IDS recolecta la información de diferentes fuentes de su red y la analiza en busca de patrones que puedan indicar violación de la seguridad alertándolo ante intentos eventuales de intrusión.

2.4.4.4 Funciones del IDS

- Supervisar la actividad del sistema y del usuario para luego analizarla en cuanto a problemas como ataques al nombre de usuario por parte de usuarios no autorizados o paquetes de información que contengan códigos malignos.
- Revisar la integridad de la información fundamental y archivos del sistema para asegurarse que los usuarios no autorizados no la han alterado.
- Inspeccionar las configuraciones del hardware y software de un sistema a fin de señalar proactivamente los aspectos vulnerables de la red como características o errores que aumenten la posibilidad de daños por acción de los hackers o accidentes.
- Buscar patrones anormales de actividad en el intercambio rutinario de la información en la red.
- Proteger un sistema operativo de toda actividad del usuario que sea una violación de las políticas de seguridad de la red. El software para la detección de intrusiones no sabe automáticamente qué constituye una violación de forma que debe configurarse de acuerdo a las políticas individuales de seguridad. Después de completar cada uno de los pasos anteriores, el software alertará si detecta una violación de la seguridad.

2.4.5 IPS (INTRUSIÓN PREVENTION SYSTEM)

Un **Sistema de Prevención de Intrusos (IPS)** es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos. La tecnología de *Prevención de Intrusos* es considerada por algunos como una extensión de los **Sistemas de Detección**

de Intrusos (IDS), pero en realidad es otro tipo de control de acceso, más cercano a las tecnologías cortafuegos.

Los IPS fueron inventados de forma independiente para resolver ambigüedades en el monitoreo pasivo de redes de computadoras, al situar sistemas de detecciones en la vía del tráfico. Los IPS presentan una mejora importante sobre las tecnologías de cortafuegos tradicionales, al tomar decisiones de control de acceso basados en los contenidos del tráfico, en lugar de direcciones IP o puertos. Dado que los IPS fueron extensiones literales de los sistemas IDS, continúan en relación.

También es importante destacar que los IPS pueden actuar al nivel de equipo, para combatir actividades potencialmente maliciosas.

La diferencia entre los sistemas de detección de intrusos y los sistemas de prevención de intrusos radica en la mayor capacidad de proactividad de éstos últimos. Si bien los sistemas de detección de intrusos actuales son capaces de interactuar con controles preventivos, tales como firewalls, para detener un ataque en progreso, esta capacidad es generalmente reactiva por lo que se clasificaría como correctiva. Los sistemas de prevención de intrusos en cambio, poseen filtros y restricciones activas desde un inicio, las cuáles se van ajustando de acuerdo con la información que proporciona el elemento analizador de estos controles (sin necesidad de que exista un ataque de por medio).

La diferencia entre un IDS y un IPS se puede entender mejor a través de una analogía. Si una persona vive en un edificio de apartamentos, dispone de dos métodos para su seguridad. El primero es contar con un guardia a la entrada de su edificio y el segundo consiste en una alarma. En el primero de los casos estamos hablando de prevención de intrusos. De acuerdo a las instrucciones que se le den al “guardia”, éste detendrá el tráfico de entrada y posiblemente interrumpirá el tráfico proveniente de dicha dirección por algún tiempo, o puede activar una alerta de que algo sospechoso está pasando.

Con los sistemas de prevención de intrusos se cuenta con la flexibilidad de

identificar ataques en progreso y elegir entre si se quieren detener inmediatamente, detener el tráfico proveniente de la fuente del ataque o simplemente monitorear el tráfico. Por otro lado, un sistema detector de intrusos actuará como una simple alarma; es decir, si se detecta una actividad anormal, el sistema emitirá una alarma y cuando sea recibida por el administrador, éste actuará en consecuencia. El IDS proporciona información acerca del ataque, pero no hay forma de reaccionar sin intervención manual.

Una característica importante de la mayor parte de los IPS es la necesidad de procesadores de alta velocidad. La velocidad del procesador permite que los paquetes sean analizados en tiempo real.

2.4.5.1 Características

- Identifica y bloquea ataques y pruebas relacionadas con protocolos y aplicaciones.
- Base de datos de más de 1,500 patrones y reglas.
- Pruebas, escaneo de puertos, interrogatorios, búsqueda de hosts.
- Ataques a vulnerabilidades de aplicaciones.
- Protección de vulnerabilidades de protocolo.
- Vigila actividades de sistemas de mensajes, chat y redes de intercambio P2P.
- Notifica al administrador o bloquea el tráfico inmediatamente.
- Interfaz de manejo sencillo, con un clic habilita o deshabilita reglas y se cambia entre detección y prevención.

2.4.6 TIPOS DE FIREWALLS PERSONALES

Estos son algunos firewalls para plataforma Windows:

2.4.6.1 ZoneAlarm

La utilidad básica de este programa es la de controlar cualquier acceso a un computador y los programas que se están ejecutando en él, actualmente se puede decir que es el arma más efectiva para evitar intrusos y virus. Una utilidad imprescindible al utilizar Internet.

Dispone de diferentes niveles de seguridad que permiten desde no ser visible en Internet hasta deshabilitar NetBios o los recursos compartidos.

Además, no consume muchos recursos, de modo que es válido para cualquier tipo de máquina.

2.4.6.2 Per Systems

El programa es una barrera de protección frente a posibles ataques, muy rápido y que consume mucho menos recursos que otros Firewalls del mercado. PER Firewall controla la ejecución y autorización de los servicios de Internet tales como los protocolos de Correo, sitios web, mensajería instantánea, así como los de redes de archivos compartidos.

Se puede configurar reglas de permisos para aplicaciones que deseen transmitir datos a través de Internet y dar o bloquear el acceso independiente a una lista de programas.

PER Firewall bloquea eficientemente cualquier intento de ataque a una PC por hackers o intrusos de la red que manipulan troyanos o backdoors a través de los puertos TCP (Transmission Control Protocol) y UDP (User Datagram Protocol).
En definitiva, es una herramienta gratuita e imprescindible para navegar con seguridad.

2.4.6.3 Agnitum Outpost Firewall

Es un potente firewall destinado a proteger un equipo de ataques externos.

Sus prestaciones permiten mantener protegido un computador contra todo tipo de amenazas en Internet, como: Cookies, publicidad intrusiva, virus de correo electrónico, de una forma sencilla y sin consumir una gran cantidad de recursos.

2.4.6.4 PortsLock

Es un firewall a nivel de usuario que controla los accesos a Windows NT/XP/2000. Una vez instalado el administrador puede asignar permisos a las conexiones, controlando que usuarios pueden acceder a los puertos TCP/IP con diferentes protocolos (STMP, POP3, FTP, HTTP, Telnet, etc) dentro de una red, pudiendo configurarse para unos determinados días de la semana u horas en el sistema.

También es posible establecer un conjunto de IP´s aceptadas o rechazadas para las conexiones con los puertos TCP/UDP.

2.4.6.5 MindSoft Firewall

Consigue una mayor sensibilidad a la hora de enfrentarse a posibles ataques y ofrece soluciones para evitarlos. Además es capaz de detectar todo tipo de virus de tipo troyano.

Permite crear distintos niveles de seguridad, realizar filtros, bloquear direcciones (conexiones), bloquear puertos remotos y locales, etc.

2.4.7 TIPOS DE ANTIVIRUS

2.4.7.1 SaveSystem

Es un completo sistema de seguridad que permite proteger el computador. Actúa en varios niveles, desde la protección clásica de un firewall para evitar ataques y problemas con la conexión, hasta en la ejecución de programas y seguridad local del computador.

Brinda una efectiva protección en los siguientes conceptos de seguridad informática:

- Protección a intentos de hackeo por red, mediante el sector "Autenticación y log-in".
- Protección de hacking al sistema operativo.
- Restricción de la cargas de nuevos programas por parte de los usuarios mediante la selección del "Nivel de Seguridad" evitando así que el computador sea infectado con virus, troyanos, gusanos y otras amenazas provenientes de los nuevos archivos instalados.
- Variada gama de ítems, para brindar una correcta protección en Internet para el navegador web "Internet Explorer" de Microsoft.
- Protección configurable bajo DOS, permitiendo entre otras las intromisiones para generar una "negación de servicio", proveniente de la eliminación de archivos, desconfiguraciones, etc.
- Completo sistema de auditoría, que mediante un historial podrá ver las acciones que realiza el usuario o el administrador del equipo.

2.4.7.2 NOD32

Es un antivirus totalmente operativo con todos los sistemas operativos de Windows. La eficacia de este antivirus contra virus, gusanos y otros códigos maliciosos es demostrada gracias a su efectiva protección incluso sobre aquellos elementos que aún no están catalogados.

Además, es mucho más rápido en la detección de virus que otros programas actuales y la eliminación de estos elementos amenazantes es mucho más segura y definitiva. El programa es actualizable periódicamente para disponer de las nuevas versiones de virus catalogadas.

2.4.7.3 SpySweeper

Es un programa bastante reconocido, ya que detecta con bastante eficacia todo tipo de elementos espías protegiéndote de accesos no autorizados, pop-ups no deseados, robos de contraseñas, troyanos y publicidad engañosa, entre otros.

Es muy sencillo de usar y no se trata de un eliminador únicamente ya que también ofrece protección en tiempo real. Las opciones de configuración del programa son muy útiles para destinar los esfuerzos solo a aquellas tareas que realmente más interesan, caso por ejemplo de un PC donde abundan las descargas.
En definitiva, se trata de un eliminador inteligente de virus espía que además ofrece a modo de encuesta todos los datos sobre los anteriores análisis realizados en tu PC.

2.4.7.4 Arovax Shield

Cada vez que se establece una conexión a Internet, muchos son los peligros que acechan la estabilidad de una PC como pueden ser los spywares, adwares, virus de cualquier índole, troyanos, bloqueadores de la página de inicio.

El programa no es un simple antivirus ya que su función más atractiva es la de actuar como barrera para que todas esas aplicaciones dañinas no consigan instalarse en la PC y hacer de las suyas. Arovax Shield actúa avisando cualquier cambio que ocurra en el sistema y que puede ser debido a que a que cualquier spyware está intentando instalar en él.

Para ello, Arovax Shield hace un escaneo y control de todas las zonas que vulnerables de ser infectadas, prestando especial atención a elementos como el fichero host, la página de inicio del navegador predeterminado, la grabación de cookies, las entradas del Registro de Windows, etc.

2.4.7.5 Trojan Remover

Estos virus que les sirven a otras personas de llave de entrada a un sistema son cada vez más comunes y adoptan las más diversas formas para no ser reconocidos. Es posible que muchos antivirus genéricos no presten la atención debida a estos programas, esta aplicación le mantendrá limpio de troyanos con seguridad. Permanecerá atento a cualquier actividad o fichero sospechoso para informar y eliminar la amenaza. Es rápido y sencillo de utilizar.

2.4.7.6 Panda Platinum Internet Sec

Es un poderoso antivirus para profesionales especializado en la protección del equipo si se utiliza Internet y el correo electrónico. El antivirus es capaz de eliminar agentes de todo tipo: Encriptados, Polimórficos, de Boot, de Fichero, de Macro, applets Java, controles Activex, etc.

El programa ofrece una completa protección al navegar por Internet eliminando virus en los más conocidos navegadores: Explorer, Netscape, Mozilla... y en la mayoría de los clientes de correo electrónico Outlook Express.

Su actualización frecuente a través de Internet le hace ser uno de los antivirus más efectivos y seguros del mercado.

2.4.7.7 Norton Antivirus

Es un producto desarrollado por Symantec destinado a mantener un computador libre de spyware, troyanos y en general cualquier virus que vulnere la estabilidad del sistema.

Gracias a su protección en tiempo real, se podrá navegar por la red con total confianza ya que avisa cada vez que el programa encuentra algo sospechoso. También es efectivo cuando se reproduce un dispositivo de almacenamiento extraíble o cuando se recibe un mail.

Algunas de las prestaciones que brinda son:

- Previene que usuarios no autorizados obtengan acceso a red.
- Provee acceso transparente hacia Internet a los usuarios habilitados.
- Asegura que los datos privados sean transferidos en forma segura por la red pública.
- Ayuda a sus administradores a buscar y reparar problemas de seguridad.
- Provee un amplio sistema de alarmas advirtiendo intentos de intromisión a su red.

CAPITULO III

SISTEMA DE SEGURIDAD PARA EL LABORATORIO DE TECNOLOGÍA DE LA INFORMACIÓN

3.1 DISEÑO DEL SISTEMA DE SEGURIDAD PARA EL LTI

El diseño de este sistema de seguridad, aportará en la preservación de la confidencialidad, integridad y disponibilidad de la información de la red, a través de la utilización de un Firewall. Es decir garantizar que solo aquellas personas autorizadas accedan a la información y a los recursos de la red, cada vez que lo requieran. Mantener la exactitud y totalidad de la información y los métodos de procesamiento.

Además, minimizará los riesgos de seguridad a los cuales está expuesta la red interna del laboratorio frente a la gran red de Internet. Reduciendo así, los riesgos de enfrentar problemas causados por cualquier tipo de virus.

En el desarrollo de este sistema se utilizará un Firewall Fortinet, de modelo: **FortiGate 60**, el cual es un dispositivo que facilita la administración de la seguridad de una red. Además incluye servicios a nivel de red como: Firewall, IPS, VPN y Traffic Shaping; y servicios a nivel de aplicación como: protección de antivirus y filtro de contenido.

El FortiGate 60 mejora la seguridad de la red, reduciendo el mal uso y abuso de la misma, y ayuda a utilizar eficientemente los recursos de comunicación sin comprometer el desempeño de la red.

El dispositivo contiene dos alternativas para su configuración y administración: Interfaz de Línea de Comandos e Interfaz de Administración basada en Web.

Este equipo presenta varias ventajas ya que dentro de la misma caja tiene las siguientes funciones:

- Antivirus Protection
- Web Content Filtering
- E-mail Filtering

- Firewall
- IPS
- VPN

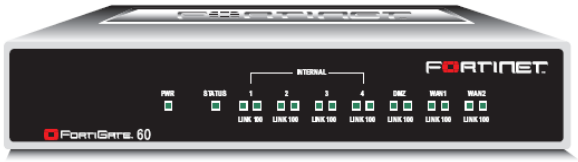


Figura 6.- Firewall FortiGate 60

3.1.1 ANÁLISIS DE LA SITUACIÓN ACTUAL DEL LTI.

El laboratorio carece de un sistema de seguridad para controlar y administrar la información de la red. Y además, la inadecuada configuración de equipos activos de red provoca lo siguiente:

- El tráfico no deseado.
- La falta de protección de la información.
- La mala administración de los servicios, tales como servidor Web, servidor de correo, servidor Active Directory.
- La falta de control en el acceso a URL's o páginas web no deseadas.
- La pérdida de software preinstalado.
- La propagación de virus y amenazas provenientes de Internet.
- La acumulación de software espía (spyware).

Como estrategia para superar los problemas existentes, se puede utilizar hardware que ayude a mejorar el control del tráfico en la red, y poder aprovechar de una mejor manera los recursos de la misma. A través de la utilización del firewall poder proteger, controlar y administrar toda la información de la red. Además por medio de pruebas, captura de paquetes, análisis de flujo de información y verificación de la configuración de equipos activos de red como switch y routers, se puede ofrecer una solución óptima para depurar y optimizar el funcionamiento de la red.

3.1.2 ESTRUCTURA FÍSICA DE RED DEL LTI ANTES DE LA IMPLEMENTACIÓN DEL SISTEMA DE SEGURIDAD.

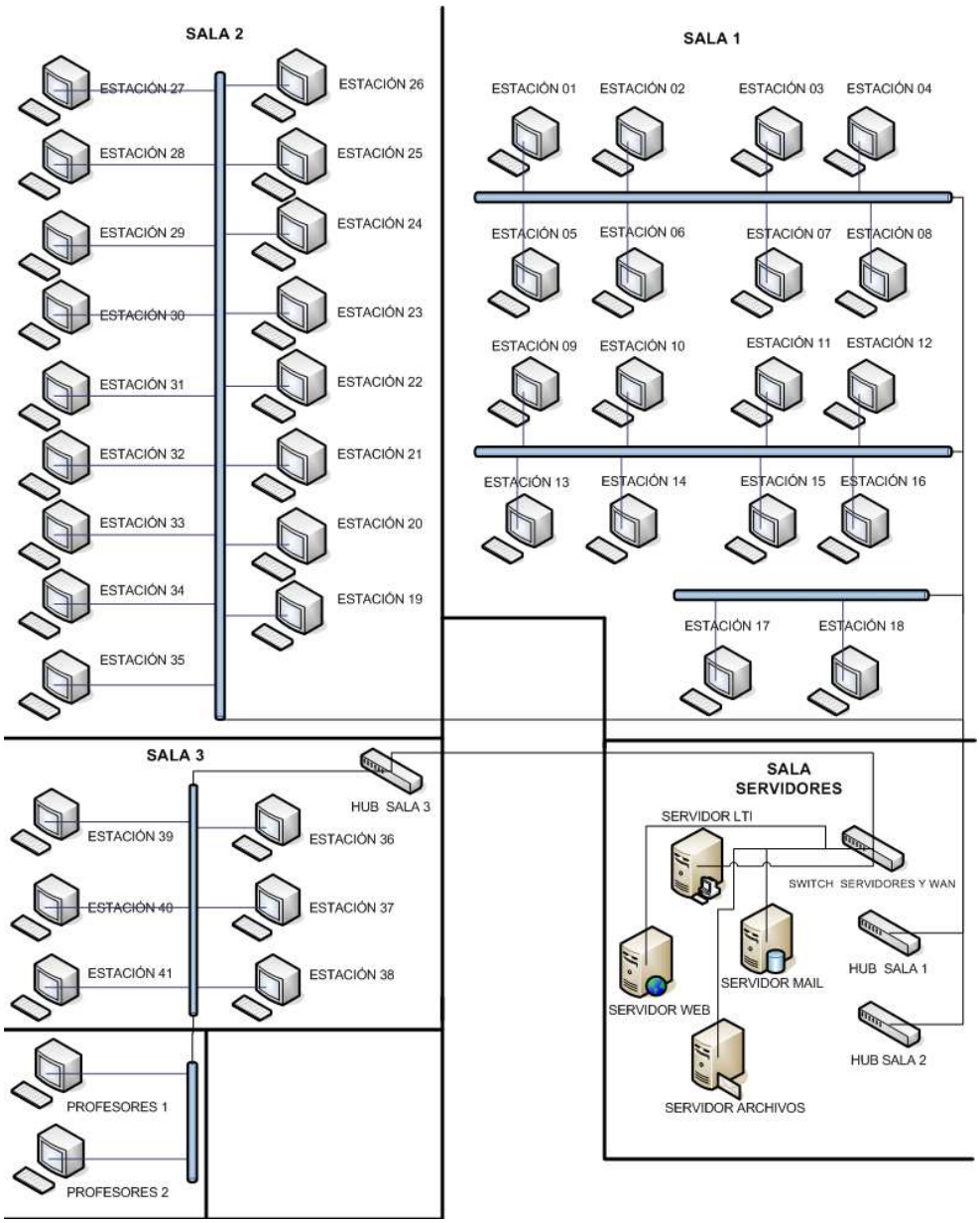


Figura 7.- Estructura de Red del LTI antes de la implementación del Firewall

3.1.3 TOPOLOGÍA DE LA RED DEL LTI IMPLEMENTADO EL SISTEMA DE SEGURIDAD CON EL FIREWALL FORTIGATE 60

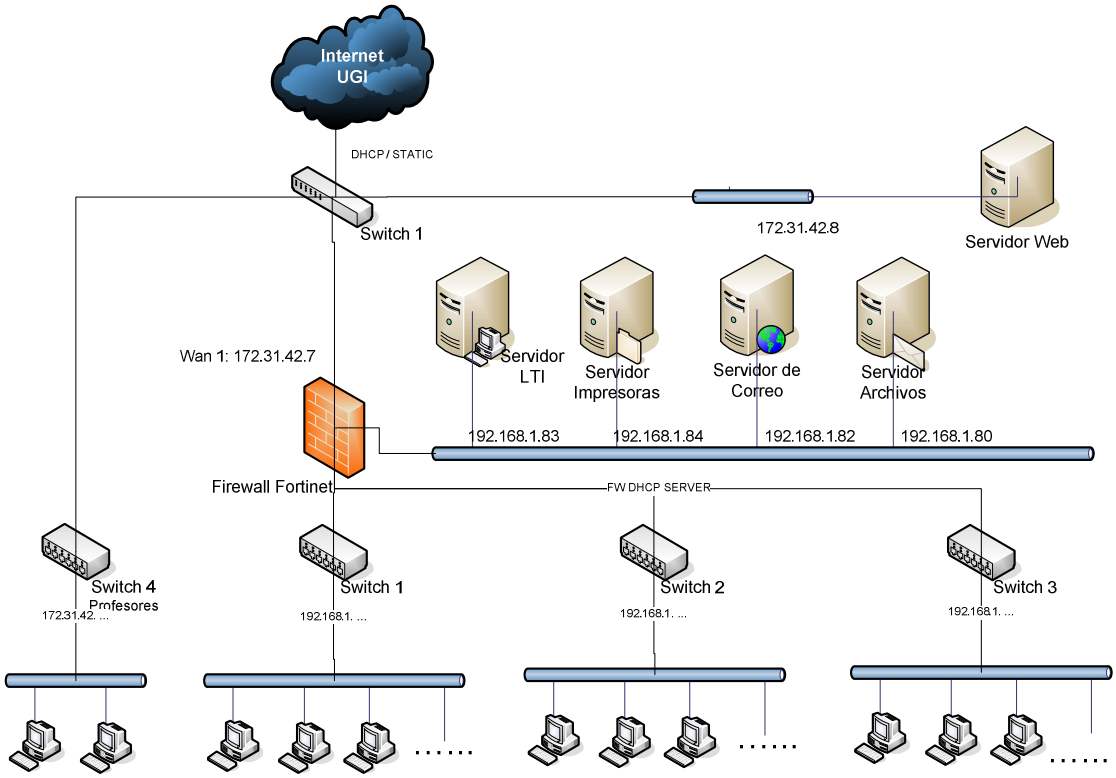


Figura 8.- Topología de Red del LTI con la implementación del Firewall

3.1.4 ALCANCE DEL SISTEMA DE SEGURIDAD

Con el desarrollo del sistema de seguridad implementado con la unidad Fortigate 60, se ha logrado estabilizar las instalaciones de software en cada una de las estaciones de trabajo y mantener un mayor control en el tráfico de Internet, logrando también el control de permisión y/o denegación de servicios a través de los protocolos de comunicación.

Este sistema, también protege toda la información que ingresa a través de navegación de Internet, como: HTTP, FTP, etc, aplicando perfiles de protección, los mismas que permiten escaneo de virus, filtro de páginas web por contenido o por URL, filtro de páginas web categorizadas por Educación, Finanzas, Entretenimiento, Pornografía, Negocios, etc, controlando el acceso a URL's no deseadas. Sin embargo, hay que destacar que hay páginas web no categorizadas, pero que han sido bloqueadas utilizando Web Filtering.

Con la implementación del FortiGate 60, se ha logrado bloquear gran cantidad de virus y de software espía, deteniendo su propagación a través de la red.

3.1.5 LIMITACIONES DE LA UNIDAD FORTIGATE 60

El modelo FortiGate 60 de Fortinet presenta limitaciones en el número de sesiones concurrentes, las mismas que se relacionan directamente con la cantidad de peticiones que emite un usuario, provocando la saturación de la red, donde el fabricante especifica que el límite de este modelo son 2000 sesiones concurrentes. En este caso, se ha comprobado, a través de varias mediciones, que difícilmente puede superarse este límite, debido al número de estaciones de trabajo y usuarios que ocupan la red (Figura 9).

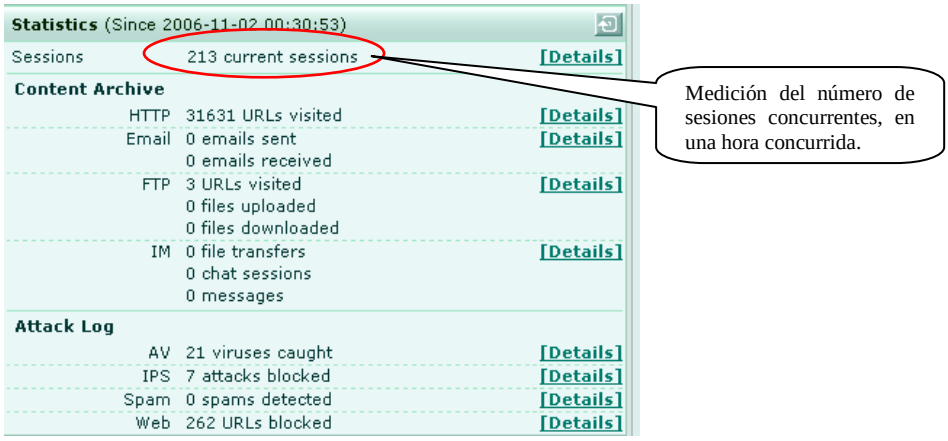


Figura 9.- Sesiones Concurrentes

El equipo viene con un año de licencia de Antivirus, IPS, Web Filtering, Spam Filtering y FortiGuard Center. La expiración de ésta, ocasiona que los servicios de seguridad del firewall no funcionen completamente, desprotegiendo toda la red.

El Módulo de ***Log&Report*** incluido en el FortiGate 60 es limitado ya que no se puede almacenar ni generar ningún tipo de reportes. Porque se necesita la implementación de otra unidad Fortinet FortiAnalizer, la misma que actúa como servidor donde almacenaría los archivos logs de reportes.

3.2 CONFIGURACIÓN DEL FIREWALL FORTIGATE 60

3.2.1 CONFIGURACIÓN INICIAL

Antes de comenzar, se necesita lo siguiente:

- Conectar cables ethernet desde el computador a un switch y luego a la unidad FortiGate 60 en la interfaz internal.
- Internet Explorer 6, Firefox 1 o Mozilla 1.6 (en adelante), también soporte Java para acceder a la consola de administración basada en web.
- Un conector DB9F-null para cable modem y un programa de emulación Terminal, (ejemplo: HyperTerminal, Minicom o TeraTerm).

3.2.1.1 Conexión de la Interfaz de Línea de Comandos (CLI)

Se puede instalar y configurar la unidad de FortiGate usando el CLI. La ventaja de utilizar esta interfaz es que los cambios de configuración son inmediatamente efectivos sin necesidad de resetear el firewall o interrumpir algún servicio.

Para conectar el FortiGate mediante la Interfaz CLI

1. Conectar el cable modem al puerto de comunicaciones del computador y el otro extremo al puerto de consola del firewall.
2. Asegurarse de que el firewall esté encendido.
3. Iniciar el programa HyperTerminal, entrando un nombre de conexión.
4. Configurar el HyperTerminal para conectar directamente al puerto de comunicaciones del computador.
5. Seleccionar los siguientes parámetros:

   Bits por Segundo: 9600

   Bits de Datos: 8

   Pariedad: No

   Bits de parada: 1

   Control de Flujo: Ninguno

6. AL conectar a la interfaz de línea de comandos del firewall, ingresar un nombre de usuario administrador. Por default es *admin*.

3.2.1.2 Conexión de la Interfaz de Administración basada en Web.

La consola de administración basada en web, presenta una interfaz más amigable, ya que es una interfaz gráfica. Permitiendo configurar y administrar con mayor facilidad este dispositivo.

Para conectar la Interfaz de Administración Basada en Web

1. Configurar las direcciones IP del computador, con la siguiente dirección IP estática: 192.168.1.2, con una máscara de subred: 255.255.255.0. O también se puede trabajar con una dirección IP dinámica usando el DHCP del FortiGate, en el rango: 192.168.1.1 a 192.168.1.254.
2. Usando el cable cruzado o un hub/switch y cables ethernet, conectar la interfaz internal de la unidad FortiGate a la tarjeta de red del computador.
3. Iniciar el navegador de Internet y buscar la dirección: https://192.168.1.99.
4. Escribir admin en el campo nombre de usuario y clic en login.

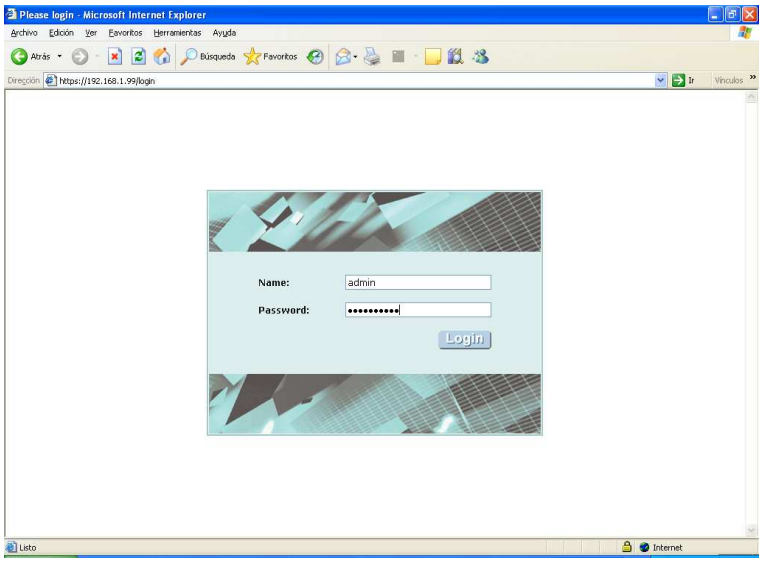


Figura 10.- Login en la Interfaz de Administración basada en Web

5. Pantalla inicial de la interfaz de administración basada en web.

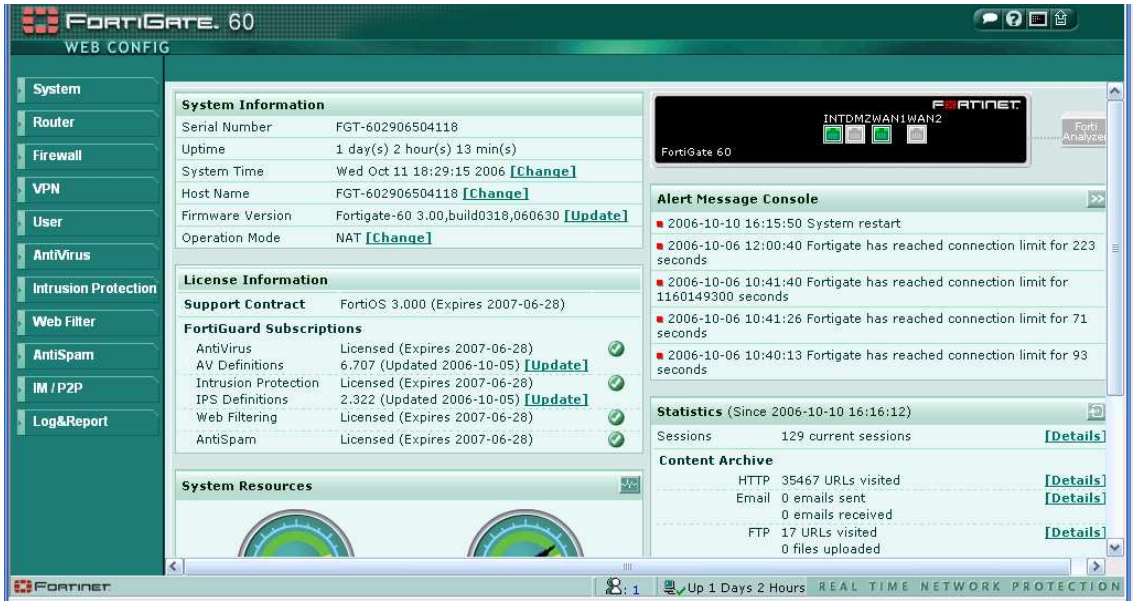


Figura 11 .- Pantalla Inicial de la Interfaz de Administración

3.2.2 MODO DE OPERACIÓN

Antes de configurar la unidad FortiGate, es necesario planificar su integración dentro de la red. Es decir, se debe decidir si se desea que la unidad sea visible a la red, qué funciones se desea que provea el firewall y cómo se desea controlar el flujo de tráfico entre las interfaces.

Esto depende de qué modo de operación se seleccione. El FortiGate puede ser configurado en uno de los dos modos: NAT o Transparent.

3.2.2.1 Modo NAT (Network Address Translation)

3.2.2.1.1 Objetivo[23]

El objetivo es cambiar la dirección origen en cada paquete de salida y, dependiendo del método, también el puerto origen para que sea único. Estas traducciones de dirección se almacenan en una tabla, para recordar qué dirección y puerto le corresponde a cada dispositivo cliente y así saber donde deben

[23] http://es.wikipedia.org/wiki/Network_Address_Translation

regresar los paquetes de respuesta. Si un paquete que intenta ingresar a la red interna no existe en la tabla de traducciones, entonces es descartado. Debido a este comportamiento, se puede definir en la tabla que en un determinado puerto y dirección se pueda acceder a un determinado dispositivo.

3.2.2.1.2 NAT/Route Mode

En el modo NAT/Route, la unidad FortiGate es visible a la red. Todas las interfaces son de subredes diferentes. Las interfaces disponibles en este modo de operación son las siguientes:

- Internal: es la interfaz de la red interna, en la cual se pueden conectar todas las subredes LAN.
- WAN 1: es la interfaz por default de la red externa, (usualmente Internet).
- WAN2: es la interfaz redundante de la red externa.
- DMZ: es la interfaz de la red de-militarizada (DMZ).

Las políticas de Firewall controlan el flujo de tráfico basándose en las direcciones de origen, las direcciones de destino y el servicio de cada paquete. En el modo NAT, el firewall realiza la traducción de las direcciones de red antes de enviar el paquete a la red de destino.

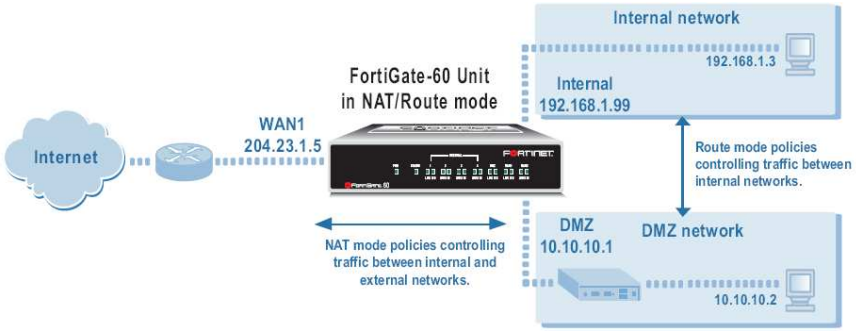


Figura 12.- Ejemplo de configuración de red con Modo NAT/Route

3.2.2.1.2 NAT/Route Mode con múltiples conexiones de redes externas

Con el Modo NAT/Route se puede configurar la unidad FortiGate con dos conexiones de red externas. Por ejemplo, se puede crear la siguiente configuración:

- WAN 1: es la interfaz por defecto de la red externa, (usualmente Internet).
- WAN 2: es la interfaz redundante de la red externa.
- Internal: es la interfaz de la red interna.

El Routing puede ser usado para redireccionar automáticamente las direcciones desde una interfaz si la conexión de red externa falla.

El modo NAT crea políticas para el control de flujo de tráfico entre la internal (red privada) y la external (red pública).

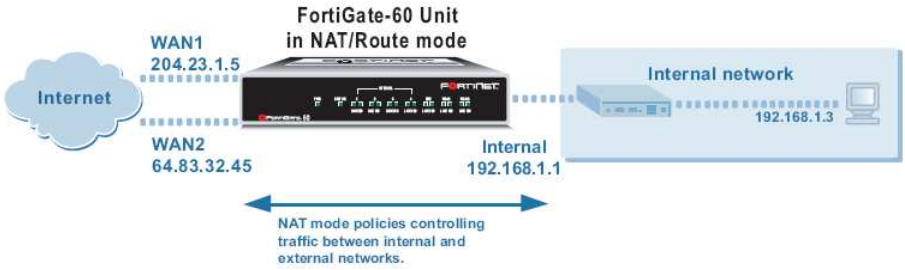


Figura 13.- Ejemplo de multiple configuración de Internet con NAT/Route

3.2.2.1.3 Modo Transparent

Por lo general, se usa la unidad FortiGate en modo transparente en una red privada detrás de un firewall existente o detrás de un router. El FortiGate realiza las funciones de un firewall, IPSec VPN, virus scanning, IPS, web content filtering y spam filtering.

En el modo Transparente, la unidad FortiGate es invisible a la red. Solo se debe configurar una dirección IP administrada, que se pueda realizar cambios de

configuración. La dirección IP administrada también es usada para actualizar definición de antivirus y ataques.

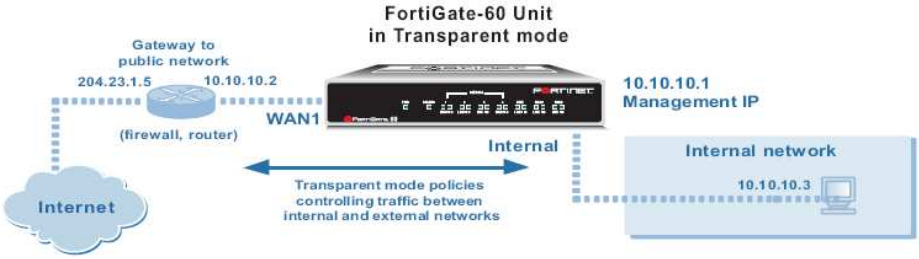


Figura 14.- Ejemplo de configuración de red en Modo Transparent

Para configurar el Modo de Operación

En este caso se recomienda trabajar en Modo NAT.

1. Sobre el menu *System* (Figura 11), seleccionar *Config*.
2. Clic en *Operation Mode*.
3. Escoger el modo de operación *NAT* (Figura 15).
4. Clic en *Apply*.

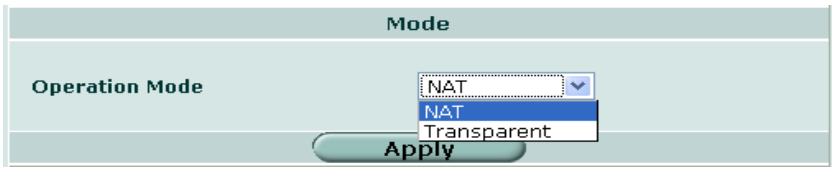


Figura 15.- Configuración de Modo de Operación

3.2.3 CONFIGURACIÓN DE INTERFACES

3.2.3.1 Configuración de Interfaz WAN 1

Se debe configurar la interfaz de red WAN1. La misma que permite la entrada y salida de Internet al resto de la red. (Figura 16).

Para configurar Interfaz Wan1

1. Sobre el menú *System* (Figura 11), ir a *Network*, luego clic en *Interface*.
2. Editar la interfaz *wan1*.

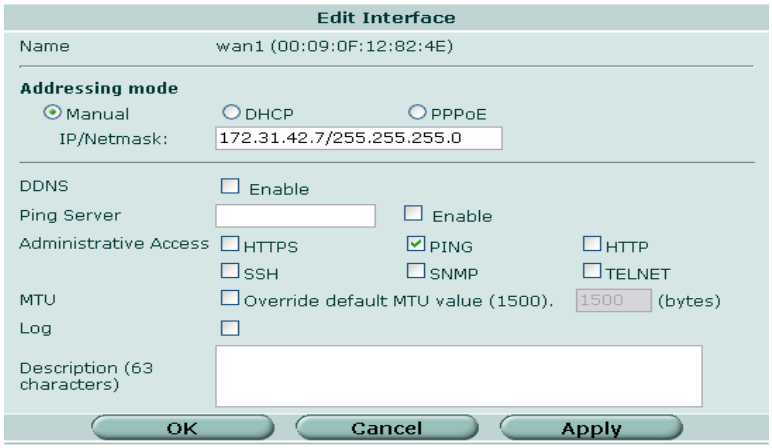


Figura 16.- Configuración de Interfaz wan1

3. En *Addressing mode*, escoger la opción *Manual*.
4. En *IP/Netmask* escribir la dirección IP pública asignada por la Unidad de Gestión de la Información (UGI) con su respectiva máscara de subred: 172.31.42.7/255.255.255.0
5. En *Administrative Access* habilitar solo la siguiente opción:

   PING: la interfaz responde al comando ping. Usar esta configuración para verificar la instalación y para pruebas.

   Nota: En el caso de habilitar el resto de protocolos: HTTPS, HTTP, SSH, SNMP, TELNET, se expondría a permitir conexiones hacia el firewall.

   HTTPS: permite conexiones seguras https para la administración del firewall a través de la consola basada en web, desde la red wan.

   HTTP: permite conexiones http para administrar el firewall a través de la consola gráfica basada en web, desde la red wan.

   SSH: permite conexiones SSH a la consola de línea de comandos, desde la red wan.

   SNMP: permite la administración remota SNMP.

   TELNET: permite conexiones Telnet a la consola de línea de comandos. Las conexiones telnet no son seguras y pueden ser interceptadas por terceras personas.
6. Para cambiar el *MTU*, habilitar *Override default MTU value (1500)*, e ingresar el tamaño MTU de 68 a 1500 bytes para modo Manual, 576 a 1500 bytes para modo DHCP y 576 a 1492 para modo PPPoE. En modo

Transparente, si se cambia el MTU para una interfaz, se debería cambiar al mismo MTU para todas las interfaces.

7. Si se desea, seleccionar *Log* para guardar los archivos logs de cualquier tráfico hacia o desde la interfaz.

3.2.3.2 Configuración de DNS

La unidad FortiGate requiere DNS para resolver nombres de host para cualquiera de estos servicios, incluyendo e-mails de alerta y bloqueo de URL.

La unidad ForitGate puede proveer reenvío de DNS.

Los requerimientos son enviados a la unidad FortiGate, los cuáles son reenviados al DNS configurado.

Para añadir una dirección de Servidor DNS

1. Sobre el menú *System* (Figura 11)**,** ir a *Network*.
2. Luego clic en *Options.*
3. Elegir la opción: *Use the following DNS Server addresses* (Figura 17).
4. Ingresar el *Primary DNS Server*, asignado por la UGI.
5. Ingresar el *Secondary DNS Server*, asignado por la UGI.
6. Habilitar el DNS para la interfaz Internal.

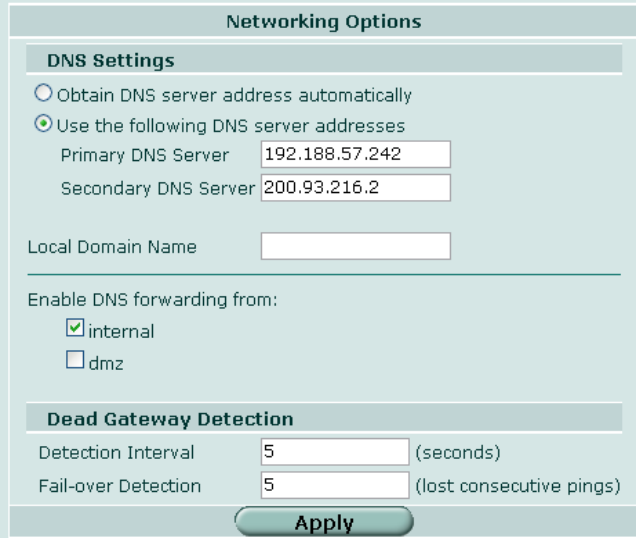


Figura 17.- Configuración de DNS

3.2.3.3 Configuración de Static Route

Modo NAT/Route

Las rutas estáticas controlan el destino del tráfico saliente de la unidad FortiGate. Se configura rutas añadiendo direcciones IP de destino y máscara de red. Entonces se añade el gateway al cual el tráfico de estas direcciones es enrutado.

La unidad FortiGate asigna rutas utilizando el mejor algoritmo de coincidencia. Para seleccionar una ruta para un paquete, la unidad FortiGate busca de una tabla, la ruta que mejor coincida con la dirección destino del paquete. Si no se encuentra coincidencia, la unidad FortiGate enruta el paquete utilizando la ruta por defecto.

Para añadir un Static Route

1. Sobre el menú *Router* (Figura 11)**,** ir a *Static*.
2. Luego clic en *Static Route*.
3. Click en *Create New*.

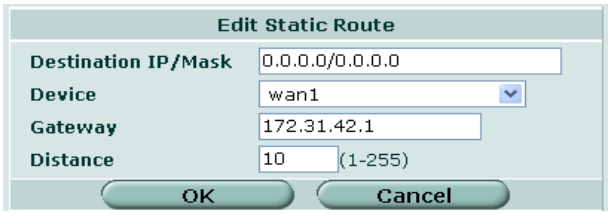


Figura 18.- Configuración de Static Route

4. En el campo *Destination IP/Mask*, ingresar la ruta de destino y la máscara. Ingresar 0.0.0.0 para la ruta por defecto.
5. Para el campo *Device* seleccionar la interfaz de FortiGate a través de la cual se enrutará el tráfico.
6. En el campo Gateway, ingresar la dirección IP de Gateway, que en este caso es: 172.31.42.1.
7. Si se requiere, en el campo *Distance*, ingresar una nueva distancia.
8. Clic en *OK*.

3.2.3.4 Configuración de Interfaz Internal

La Interfaz Internal permite conectar al firewall la red o subredes LAN del laboratorio. Además, a través de éste, se podrá tener acceso a Internet. Ver Figura 18.

Para configurar Interfaz Internal

1. Sobre el menú *System* (Figura 11), ir a *Network*.
2. Luego clic en *Interface*.
3. Editar la interfaz *Internal*.

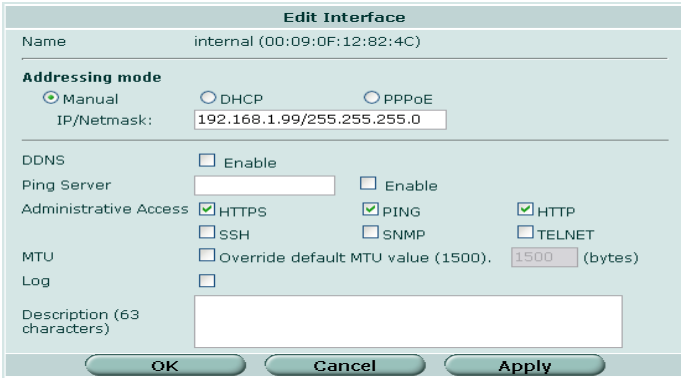


Figura 19.- Configuración de Interfaz Internal

4. En *Addressing mode*, escoger la opción *Manual* (Figura 19).
5. En *IP/Netmask* mantener la dirección IP y su respectiva máscara de subred designadas por defecto: 192.168.1.99/255.255.255.0.
6. En *Administrative Access* seleccionar los tipos de acceso administrativo permitidos para esta interfaz.

   HTTPS: permite conexiones seguras https para la administración del firewall a través de la consola basada en web.

   HTTP: permite conexiones http para administrar el firewall a través de la consola gráfica basada en web.

   SSH: permite conexiones SSH a la consola de línea de comandos.

   SNMP: permite la administración remota SNMP.

   TELNET: permite conexiones Telnet a la consola de línea de comandos. Las conexiones telnet no son seguras y pueden ser interceptadas por terceras personas.
7. Para cambiar el *MTU*, habilitar *Override default MTU value (1500)*, e ingresar el tamaño MTU de 68 a 1500 bytes para modo Manual, 576 a 1500 bytes para modo DHCP y 576 a 1492 para modo PPPoE. En modo Transparente, si se cambia el MTU para una interfaz, se debería cambiar al mismo MTU para todas las interfaces.
8. Si se desea, seleccionar *Log* para guardar los archivos logs de cualquier tráfico hacia o desde la interfaz.

3.2.3.5 Configuración del DHCP

En este caso se recomienda habilitar el *DHCP Server*, en la interfaz *Internal*.

También se recomienda, utilizar la opción *Unlimited* en el campo *Lease Time*, para que la dirección IP de cada estación de trabajo asignada por el DHCP del Fortinet, sea de tiempo indefinido.

Para configurar el DHCP

1. Sobre el menú *System* (Figura 11)**,** ir a *DHCP*.
2. Expandir la interfaz *Internal*.
3. Expandir *Servers*.
4. Editar *internal_dhcp_server*.
5. Clic en *Enable* (Figura 20).
6. En el campo *Type* escoger *Regular*.
7. En el campo *IP Range* escoger el rango direcciones IP dinámicas.
8. En *Network Mask* ingresar la máscara de red que corresponda a la clase de red ingresada en el rango de direcciones.
9. En *Default Gateway* ingresar la dirección IP configurada en la interfaz Internal: 192.168.1.99.
10. En el campo *Lease Time* escoger la opción *Unlimited*.

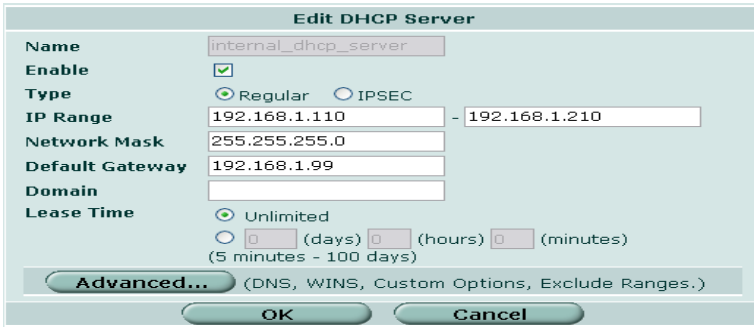


Figura 20.- Configuración de DHCP

3.2.4 FIREWALL

3.2.4.1 Políticas de Firewall

Una política de Firewall es un conjunto de instrucciones usadas por la unidad FortiGate para decidir qué hacer con las conexiones requeridas. Cuando el Firewall recibe una petición de conexión en forma de paquete, éste analiza el paquete para extraer la dirección de origen, la dirección de destino y el servicio por su número de puerto.

Para el paquete que debe ser conectado a través de la unidad FortiGate, una política de firewall debe estar en el sitio que coincida la dirección origen, la dirección destino y el servicio de dicho paquete. La política direcciona la acción del firewall sobre el paquete. Esta acción puede ser la de permitir la conexión, denegar la conexión, requerir autenticación previa a la conexión que es permitida, o también procesar el paquete como un IPSec VPN. También se pueden añadir horarios a las políticas así el firewall puede procesar conexiones diferentemente dependiendo de la hora del día, o del día de la semana, mes o año.

Cada política puede ser individualmente configurada para enrutar conexiones o aplicar NAT para trasladar direcciones IP de origen y destino y puertos. Se pueden añadir pilas de IP's para usar NAT dinámico cuando el firewall traslada direcciones de origen. Se puede usar políticas para configurar PAT's (Ports Address Translation) a través de la unidad FortiGate.

- Se puede añadir perfiles de protección (protection profiles) a las políticas para aplicar ***antivirus protection***, ***web filtering*** y ***spam filtering to web***, ***email services*** y ***file transfer***.

3.2.4.2 Registro de Direcciones

Se puede añadir, editar y borrar las direcciones firewall como se requiera. También se puede organizar las direcciones relacionadas dentro de grupos de direcciones para simplificar la creación de políticas.

Una dirección de firewall puede ser configurada con un nombre, una dirección IP, una máscara de red, o un nombre y un rango de dirección IP.

Para añadir una dirección

1. Sobre el menú *Firewall*, seleccionar *Address* y luego clic en *Create New*.
2. Ingresar el nombre de la dirección sin espacios.

Figura 21.- Registro de Direcciones

3. En el campo *Subnet / IP Range*:
   - Para ingresar una dirección IP, ingresar solo la dirección y su respectiva máscara de red se asignará automáticamente. Por ejemplo: 192.168.1.127.
   - Para ingresar un rango de direcciones IP, hacerlo en el siguiente formato: 192.168.1.110-192.168.1.210.
4. Clic en *OK*.

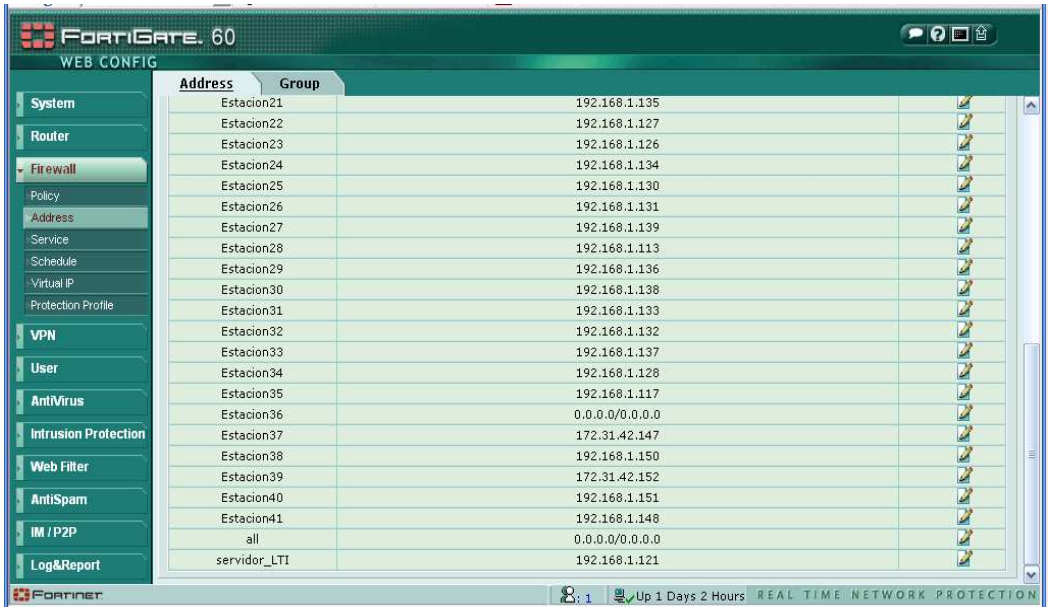


Figura 22.- Todas las direcciones IP registradas

3.2.4.3 Grupos de Direcciones

Se puede organizar direcciones relacionadas dentro de grupos de direcciones para facilitar la configuración de políticas.

Para crear un grupo de direcciones

1. Sobre el menú *Firewall* (Figura 11), seleccionar *Address*.
2. Ir a la pestaña *Group*, clic en *Create New*.
3. Ingresar un nombre de grupo sin espacios (Figura 23).
4. Seleccionar las direcciones de la lista de *Available Address* y usar la flecha ↓ para mover a la lista *Members*.
5. Clic en *OK*.

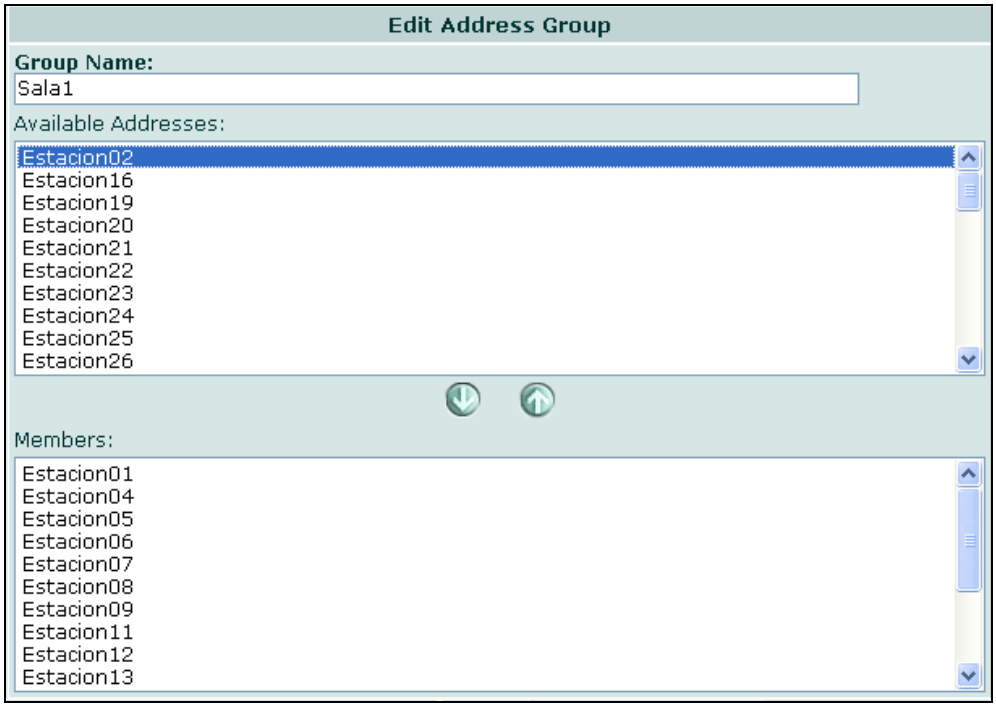


Figura 23.- Grupos de Direcciones

3.2.5 SCHEDULES (INTERVALOS DE TIEMPO)

Se usa intervalos de tiempo para controlar cuando las políticas son activas o inactivas. Se puede crear on-time schedules (intervalo en un tiempo) o recurring schedules (intervalos recurrentes).

3.2.5.1 On-Time Schedules

Se puede usar on-time schedules para crear políticas que son efectivas una vez para el período de tiempo especificado en el intervalo.

Se puede crear un On-Time Schedule que activa o desactiva una política para un período de tiempo específico.

Para configurar On-Time Schedule

1. Sobre el menú *Firewall* (Figura 11), seleccionar *Schedule*
2. En la pestaña *One-time*, clic en *Create New*
3. Ingresar un nombre para el Schedule (Figura 24).
4. Seleccionar en Start el año, mes, día, hora y minuto de inicio para un intervalo de tiempo.
5. Seleccionar en Stop el año, mes día, hora y minuto de finalización del intervalo de tiempo.

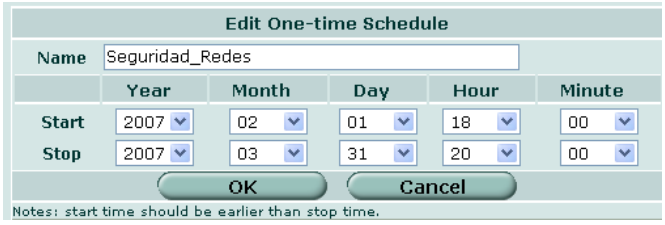


Figura 24.- Configuración de On-Time Schedule

6. Clic en *OK*.

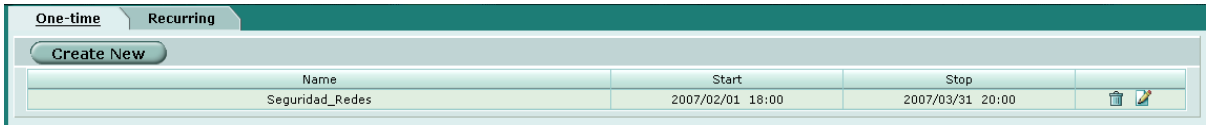


Figura 25.- Lista de On-Time Schedules creados

3.2.5.2 Recurring Schedules

Se puede crear un recurring schedule que activa o desactiva políticas a un tiempo específico del día o en un día específico de la semana. Por ejemplo, se puede

prevenir la ejecución de juegos durante horas laborables creando un recurring Schedule.

Para configurar Recurring Schedule

1. Sobre el menú *Firewall* (Figura 11), seleccionar *Schedule*.
2. Ir a la pestaña *Recurring*, clic en *Create New*.
3. Ingresar un nombre para el Schedule (Figura 26).
4. Seleccionar los días de la semana sobre los cuáles el schedule estaría activo.
5. Seleccionar una hora y minuto de inicio.
6. Seleccionar una hora y minuto de finalización.

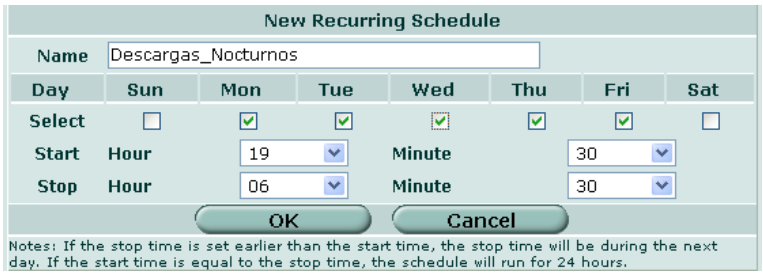


Figura 26.- Configuración de Recurring Schedule

7. Clic en *OK*.

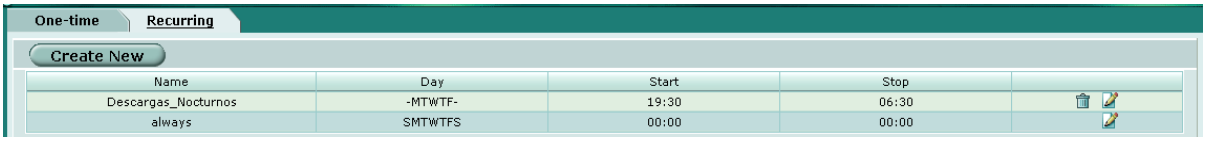


Figura 27.- Lista de Recurring Schedules creados

Nota: Para habilitar estos schedules, se lo debe hacer aplicando una política de firewall[24].

[24] Véase en Políticas de Firewall

3.2.6 SERVICIOS

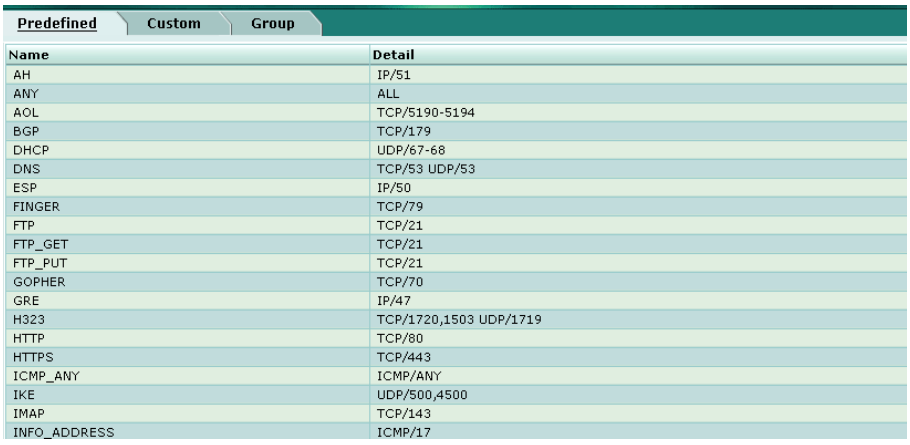
Los servicios se usan para determinar los tipos de comunicaciones aceptadas o denegadas por el firewall. Se puede añadir a una política, cualquiera de los servicios predefinidos. O también se puede crear servicios personalizados y añadir estos a un grupo de servicios.

3.2.6.1 Servicios Predefinidos

Los servicios predefinidos están incluidos por defecto en la versión de firmware de la unidad FortiGate 60.

Para ver la lista de servicios predefinidos

1. Sobre el menú *Firewall* (Figura 11), Clic en *Service*.
2. Clic en la pestaña *Predefined*.



Name	Detail
AH	IP/51
ANY	ALL
AOL	TCP/5190-5194
BGP	TCP/179
DHCP	UDP/67-68
DNS	TCP/53 UDP/53
ESP	IP/50
FINGER	TCP/79
FTP	TCP/21
FTP_GET	TCP/21
FTP_PUT	TCP/21
GOPHER	TCP/70
GRE	IP/47
H323	TCP/1720,1503 UDP/1719
HTTP	TCP/80
HTTPS	TCP/443
ICMP_ANY	ICMP/ANY
IKE	UDP/500,4500
IMAP	TCP/143
INFO_ADDRESS	ICMP/17

Figura 28.- Lista de Servicios Predefinidos

3.2.6.2 Servicios Personalizados

Se puede añadir un servicio personalizado en caso de que se necesite crear una nueva política para un servicio que no esté en la lista de los predefinidos.

Para agregar un servicio personalizado TCP o UDP

1. Sobre el menú *Firewall* (Figura 11), clic en *Service*.
2. Seleccionar el protocolo *TCP* o *UDP* de la lista.
3. Sobre la pestaña *custom*, clic en *Create New*.

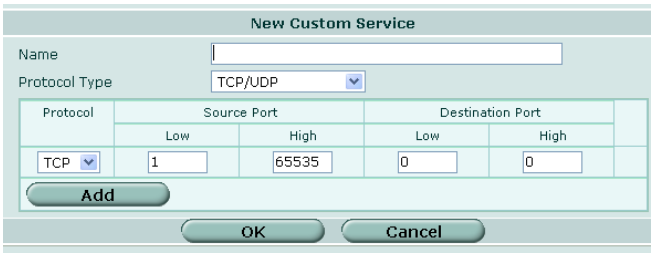


Figura 29.- Creación de Servicio Personalizado TCP/UDP

4. Ingresar el nombre del servicio, en el campo *Name*.
5. Ingresar el número de puerto en *Low and High Source Port numbers*. Si solo se usa un puerto se debe ingresar el mismo número en ambos campos.

6. Ingresar el número de puerto en *Low and High destination Port numbers*. Si solo se usa un puerto se debe ingresar el mismo número en ambos campos.
7. Clic en *OK*

Para agregar un servicio personalizado ICMP

1. Sobre el menú *Firewall* (Figura 11), clic en *Service*.
2. Seleccionar el protocolo *ICMP* de la lista.
3. Sobre la pestaña *Custom*, clic en *Create New*.

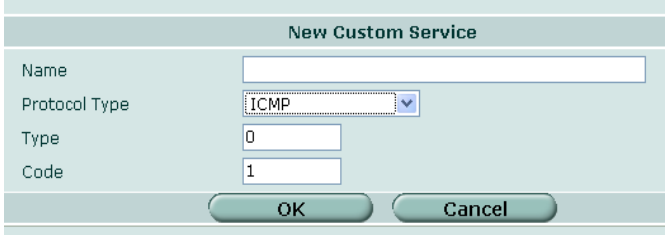


Figura 30.- Creación de un Servicio Personalizado ICMP

4. Ingresar el nombre del servicio, en el campo *Name*.
5. Ingresar el tipo de número de *ICMP* para el servicio, en el campo *Type*.
6. Si es necesario, ingresar el número de código de *ICMP* para el servicio, en el campo *Code*.
7. Clic en *OK*.

Para agregar un servicio personalizado IP

1. Sobre el menú *Firewall* (Figura 11), clic en *Service*.
2. Seleccionar el protocolo *IP* de la lista.
3. Sobre la pestaña *Custom*, clic en *Create New*.

Figura 31.- Creación de un Servicio Personalizado IP

4. En el campo *Name*, ingresar el nombre del servicio.
5. Ingresar el número de Protocolo IP para el servicio, en el campo *Protocol Type*.
6. Clic en *OK*.

3.2.6.3 Grupos de Servicios

Para facilitar el añadir políticas, se puede crear grupos de servicios y luego añadir una política para proveer o bloquear acceso para todos los servicios en el grupo. Un grupo de servicios puede contener servicios predefinidos y personalizados en cualquier combinación. Pero no se puede añadir grupos de servicios en otros grupos.

Para configurar un grupo de servicios

1. En el menú *Firewall* (Figura 11), clic en *Services*.

2. En la pestaña *Group*, clic en *Create New*.

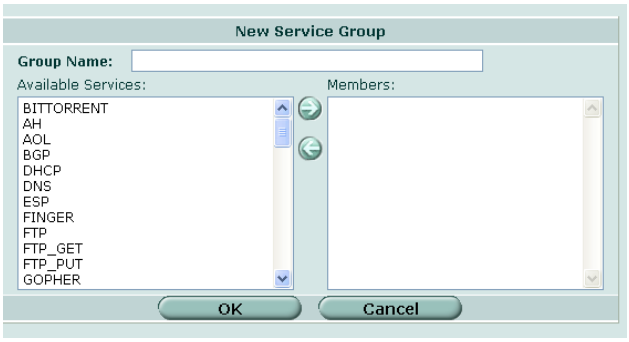


Figura 32.- Configuración de un Grupo de Servicios

3. En el campo *Group* Name, ingresar un nombre de grupo sin espacios.
4. Seleccionar desde la lista *Available Services* y usar la flecha → para mover a la lista *Members*.
5. Clic en *OK*.

3.2.7 POLÍTICAS DE FIREWALL

Cuando la unidad FortiGate recibe un requerimiento de conexión hacia una interfaz, ésta debe seleccionar de una lista de políticas aquella que coincida con el requerimiento de conexión. La unidad FortiGate elige de la lista de políticas en función de la dirección de origen y destino del requerimiento de conexión.

La unidad FortiGate entonces empieza a buscar desde el inicio de la lista de políticas hacia abajo, la primera que coincida con la dirección origen y destino del requerimiento de conexión, puerto de servicio, tiempo y fecha de la cual el requerimiento de conexión fue recibido. La primera política que coincide es aplicada para el requerimiento de conexión. Si no coincide ninguna política, la conexión es abandonada.

La política por defecto “all” acepta todos los requerimientos de conexión desde redes internas hacia Internet. Desde la red interna, los usuarios pueden navegar en la web, usar POP3 para obtener e-mails, usar FTP para descargar archivos a través del firewall, etc. ***Sí la política por default está al inicio de la lista de políticas internal -> external, el firewall permite todas las conexiones desde***

la red internal hacia el Internet debido a que todas las conexiones coinciden con las políticas por default. Sí se especifican más políticas y son añadidas a la lista a continuación de la política por defecto, entonces éstas nunca tomarán efecto.

Una política que es una excepción a la política por defecto, por ejemplo, una política para bloquear conexiones FTP, debe ser ubicada antes de la política por defecto en la lista de políticas internal -> external. En este ejemplo, todos los requerimientos de conexión FTP desde la red internal deberían entonces coincidir con la política FTP y ser bloqueados. Los requerimientos de conexión de todos los otros tipos de servicios no deberían coincidir con la política FTP pero estos deberían coincidir con la política por defecto. A pesar de esto, el firewall debería aún aceptar a todas las otras conexiones desde la red internal.

Nota: Las políticas que requieren autenticación deben ser añadidas a la lista de políticas antes de las políticas que no lo requieren; caso contrario, la política que no requiere autenticación es seleccionada primera.

3.2.7.1 Autenticación

La autenticación requiere a los miembros de un grupo de usuarios ingresar un nombre de usuario y contraseña previo a que el firewall acepte la conexión. Previo a la selección de autenticación se debe añadir un grupo de usuarios.

Se puede seleccionar la autenticación para cualquier servicio. Los usuarios pueden autenticarse con el firewall utilizando HTTP, TELNET o FTP. Para que los usuarios estén habilitados para autenticarse, se debe añadir una política HTTP, TELNET O FTP, que esté configurada para autenticación.

Se deben crear grupos de servicios que incluyan servicios específicos, por ejemplo POP3 o IMAP si se quiere que los usuarios se autentiquen para usar estos otros servicios. Los usuarios entonces, se autentican con la política utilizando HTTP, TELNET o FTP previo a la utilización de otro servicio.

Hay que asegurar que los usuarios puedan utilizar el DNS a través del firewall sin autenticación. Si el DNS no está disponible los usuarios no pueden conectarse a los servidores de web, ftp o telnet utilizando un nombre de dominio.

3.2.7.2 Secuencia de Políticas

Las políticas deberían ser listadas desde lo específico hacia lo general.

En el ejemplo a continuación, la política “all” será la última en ejecutarse, porque el resto de políticas específicas que la anteceden actuarán antes que ésta.

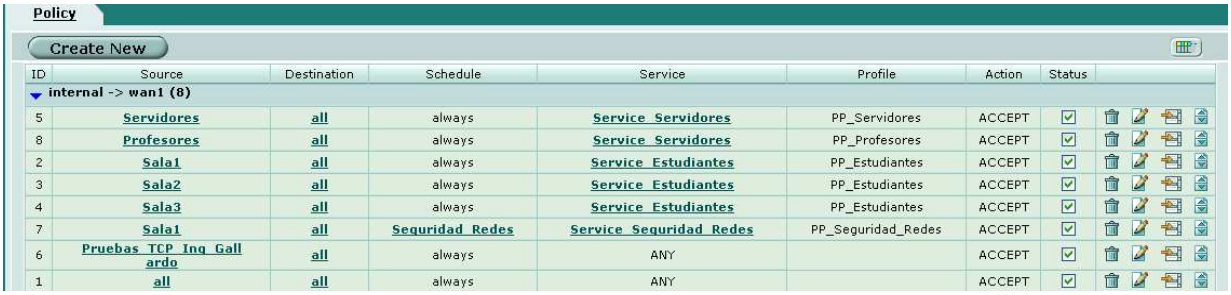


Figura 33.- Secuencia de Políticas

Las políticas de encripción estarán siempre al inicio, antes de cualquier política general.

Para configurar una Política de Firewall

1. En el menú *Firewall* (Figura 11), clic en *Policy*.
2. Clic en *Create New*.

Figura 34.- Creación de una Política de Firewall

3. Seleccionar en el campo *Source Interface/Zone*, una interfaz desde la lista.

4. Seleccionar para el campo *Address Name*, un nombre o grupo de direcciones, desde la lista.
5. Luego, seleccionar en el campo *Destination Interface/Zone*, una interfaz desde la lista.
6. Seleccionar para el campo *Address Name*, un nombre o grupo de direcciones, desde la lista.
7. Si es el caso seleccionar un *Schedule*.
8. Seleccionar en el campo service, un servicio o grupo de servicios desde la lista.
9. En el campo *Action*, seleccionar una acción desde la lista. Dependiendo de la acción seleccionada, se presentarán diferentes opciones para el resto de política.

Completando una Política ACCEPT

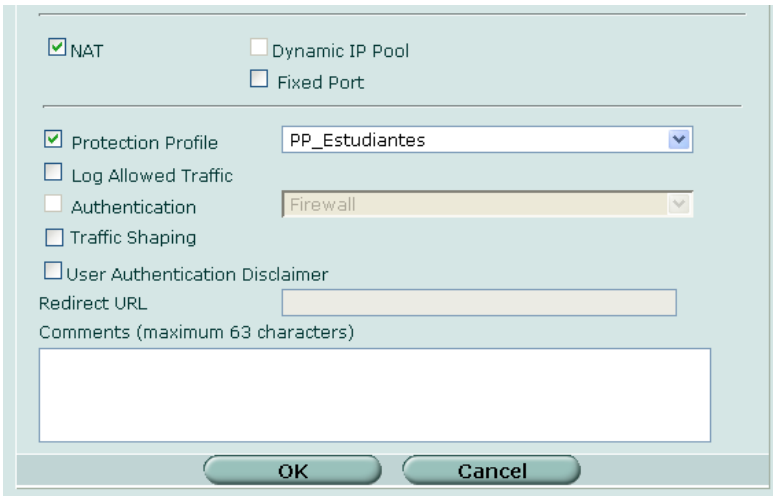


Figura 35.- Completando una Política Accept

1. Si se requiere, habilitar *NAT* (Figura 35).
2. Si se requiere, chequear la opción *Dynamic IP Pool* para seleccionar direcciones IP en forma aleatoria desde una pila.

Nota: No se puede seleccionar *Dynamic IP Pool*, si la interfaz destino o la sub-interfaz VLAN está configurada utilizando DHCP o PPPoE.

3. Si se requiere, seleccionar *Fixed Port*.

Nota: Si se selecciona *Fixed Port*, se debe también seleccionar *Dynamic IP Pool* y añadir un rango de direcciones de una pila IP dinámica a la interfaz de destino de la política. Si no se selecciona *Dynamic IP Pool*, una política con *Fixed Port* seleccionado puede solamente permitir una conexión a la vez para este puerto o servicio.

4. Habilitar *Protection Profile*, y seleccionarlo de la lista.
5. Si se requiere, elegir *Log Allowed Traffic* para habilitar el registro del tráfico.
6. En caso de que se hayan creado grupos de usuarios, se debe habilitar el campo *Authentication*, y escoger desde la lista el nombre de grupo de usuarios creado.

Completando una Política DENY

1. Si se requiere, elegir *Log Violation Traffic* para habilitar el registro del tráfico.
2. Si se requiere añadir comentarios.
3. Clic en *OK*.

Figura 36.- Completando una Política Accept

3.2.8 PROTECTION PROFILES (PERFILES DE PROTECCIÓN)

Protection Profiles permiten el control de lo siguiente:

- El tipo de tráfico protegido en:
  - HTTP
  - FTP
  - IMAP
  - POP3
  - SMTP
- El tipo de antivirus y la habilitación del intrution protection.
- El tratamiento de e-mails fragmentados y archivos sobre-pesados o e-mails.

Configurando un protection profile, permite seleccionar los protocolos a ser inspeccionados e instruir a la unidad FortiGate sobre temas relacionados como autenticaciones y cuarentenas.

La configuración de protection profile se incluye para Web Filtering, Web Category Filtering, Spam Filtering y el Intrusion Prevention System.

Protocolo	**Comportamiento**
HTTP	La página es reemplazada con otra personalizada.
FTP	Error en la sesión.
IMAP	Se remueve el adjunto y envía un mensaje personalizado.
POP3	Se remueve el adjunto y envía un mensaje personalizado.
SMTP	Error en la sesión.

Tabla 1.- Los protocolos son manipulados diferentemente cuando un virus es detectado

La unidad FortiGate incluye cuatro protection profiles por defecto:

- Strict
- Scan
- Web
- Unifiltered

3.2.8.1 Strict Protection Profile

Se usa este perfil para aplicar máxima protección del contenido a: HTTP, FTP, IMAP, POP3 y el contenido del tráfico en SMTP. No se necesita usar el strict protection profile bajo circunstancias normales, pero éste, está disponible cuando se tiene problemas extremos con virus y cuando se requiere una máxima protección en la exploración del contenido.

3.2.8.2 Scan Protection Profile

Usar este protection profile para aplicar antivirus examinando el contenido del tráfico a: HTTP, FTP, IMAP, POP3 y SMTP. La Cuarentena (Quarantine) también está seleccionada para todos los servicios de contenido.

3.2.8.3 Web Protection Profile

Este perfil se usa para aplicar antivirus examinando y bloqueando el contenido web para HTTP. Se puede añadir este perfil a las políticas de firewall que controlan el tráfico en HTTP.

3.2.8.4 Unfiltered Protection Profile

Se debe usar este profile si no se desea aplicar ninguna protección al contenido del tráfico. Se puede añadir este profile a las políticas del firewall para conexiones entre redes altamente confiables o seguras donde el contenido no necesita ser protegido.

Para Configurar un Protection Profile

1. En el menú *Firewall* (Figura 11), seleccionar *Protection Profile*.
2. En la pestaña *Group*, clic en *Create New*.
3. Ingresar un nombre de protection profile sin espacios.

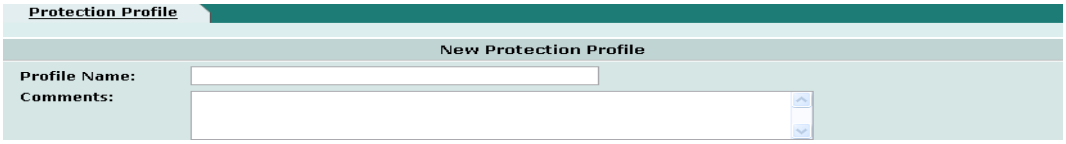


Figura 37.- Creación de un Protection Profile

4. En la opción Anti-Virus, habilitar todos los puertos donde se desee escanear antivirus.

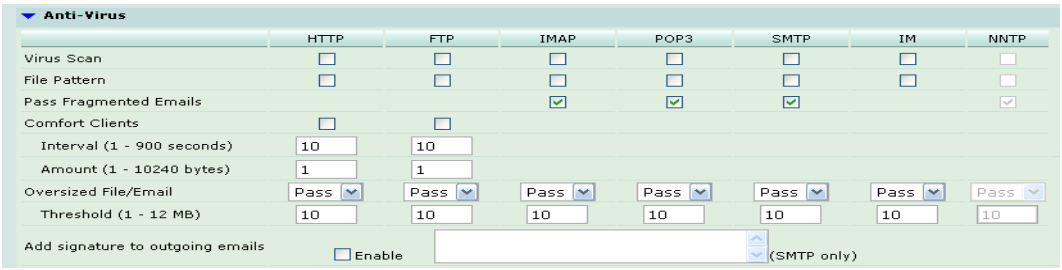


Figura 38.- Configuración de Antivirus en un Protection Profile

5. En Web Filtering, habilitar las opciones que se hayan configurado para el contenido web.

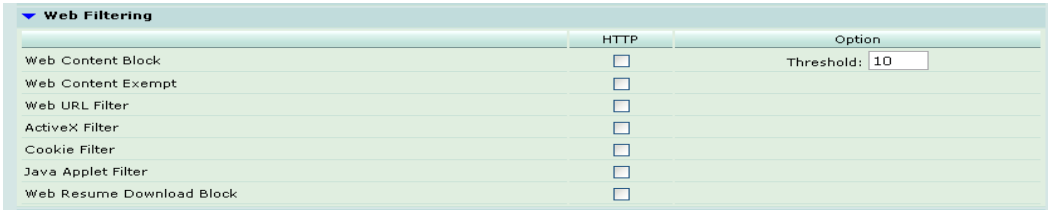


Figura 39.- Configuración de Web Filtering en un Protection Profile

6. Habilitar FortiGuard Web Filtering[25].

[25] Véase en FortiGuard Center

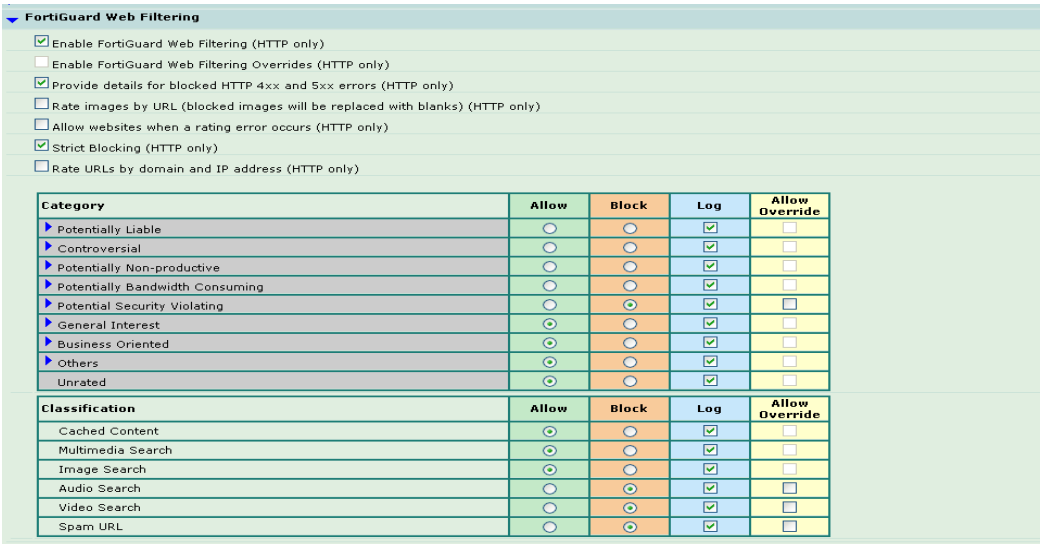


Figura 40.- Habilitar FortiGuard Web Filtering en un Protection Profile

7. En Spam Filtering, habilitar los campos según criterio personal.

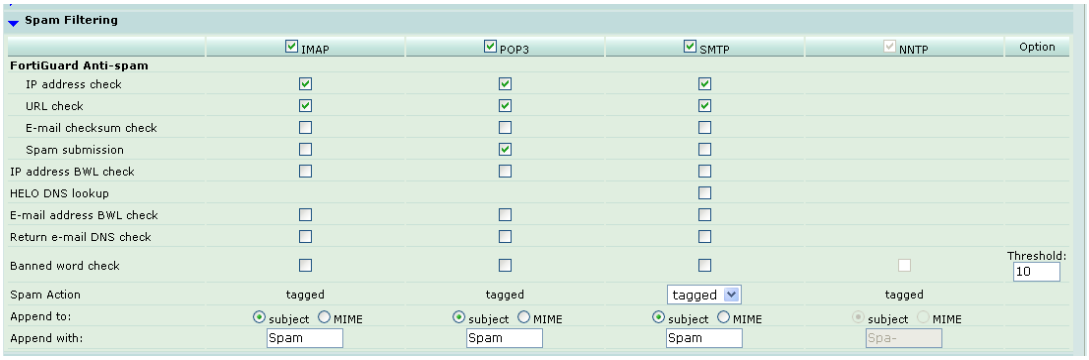


Figura 41.- Configuración de Spam Filtering en un Protection Profile

8. Habiltar IPS, Content Archive, IM/P2P.

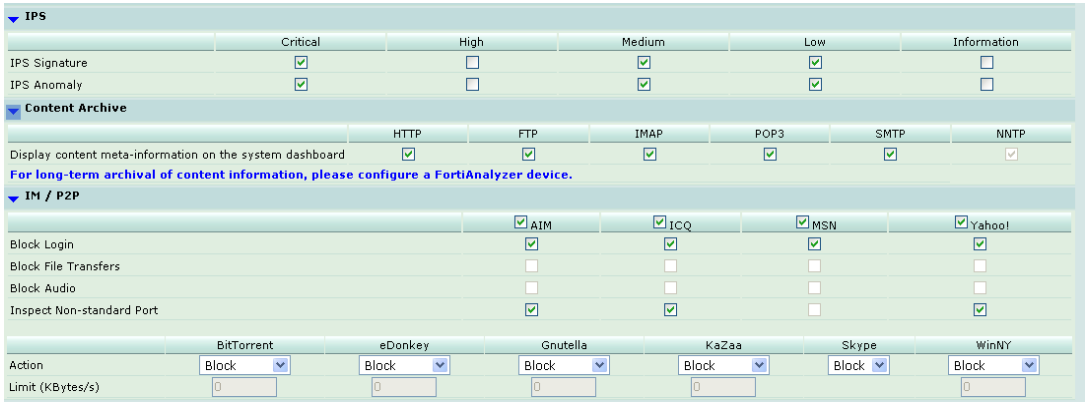


Figura 42.- Configuración de IPS, Content Archive, IM/P2P en un Protection Profile

9. Si se desea habilitar el campo de Log para cada opción del protection profile.

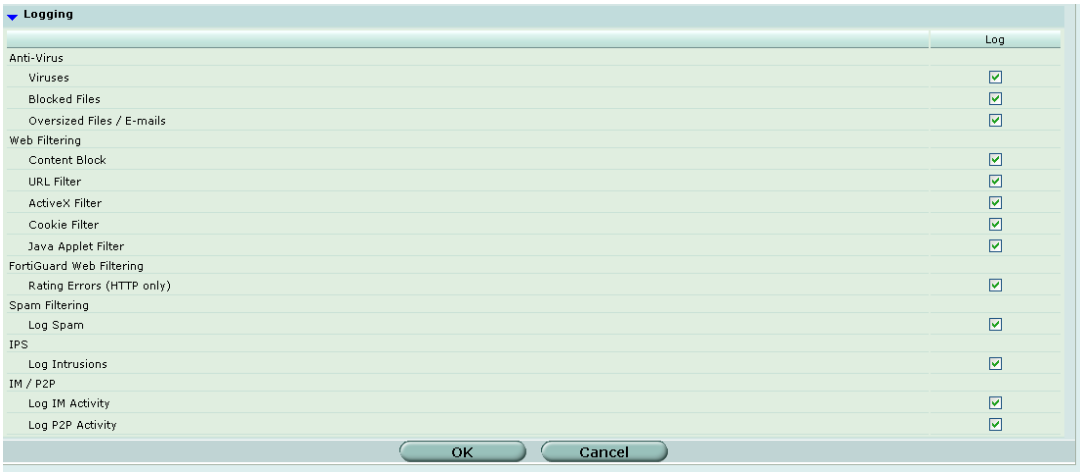


Figura 43.- Habilitar Logging en un Perfil de Protección

10. Clic en *OK*.

3.2.9 AUTENTICACIÓN DE USUARIOS

La unidad FortiGate soporta 3 diferentes tipos de usuarios / autenticaciones

- Usuario Local.
  - Nombres de Usuario y Contraseñas
- Usuarios almacenados sobre servidores *RADIUS*.
  - Nombres de Usuario y Contraseñas
- Usuarios almacenados en su directorio *LDAP*.
  - Nombres de Usuario y Contraseñas

Para que sean efectivos, estos usuarios deben estar ubicados en grupos. Solamente los grupos pueden ser utilizados para autenticación. El nombre de un grupo debe ser elegido cuidadosamente para una fácil identificación de los usuarios y en función del grupo. Múltiples grupos pueden ser creados.

El soporte a *RADIUS* debe ser configurado previamente a que pueda ser seleccionado para la autenticación de un usuario. Cuando la autenticación de

RADIUS es utilizada el nombre de usuario y contraseña son validadas sobre un servidor *RADIUS*. Si se encuentra una coincidencia la conexión es permitida. Si no existe coincidencia, la conexión es abandonada.

El soporte a *LDAP* debe ser configurado previamente a que pueda ser seleccionado para la autenticación de un usuario. Cuando la autenticación de *LDAP* es utilizada el nombre de usuario y contraseña son validadas sobre un servidor *LDAP*. Si se encuentra una coincidencia la conexión es permitida. Si no existe coincidencia, la conexión es abandonada.

Si un grupo de usuarios contiene nombres de usuarios, servidores RADIUS y servidores LDAP la unidad FortiGate lo revisa en el orden en el cual ellos fueron añadidos al grupo de usuarios.

3.2.9.1 Usuarios Locales

Los usuarios locales pertenecen únicamente a la unidad FortiGate 60. La creación de estos usuarios locales permite habilitar en las políticas de firewall, autenticaciones para el uso de los servicios HTTP y HTTPS, para esto se requiere lo siguiente:

- Toda acción dentro de una política de Firewall esté configurada como *ACCEPT*
- Configuración de *IPSEC FASE1*, 2 Túneles de Navegación VPN.

Para agregar un Usuario Local

1. Sobre el menú *USER* (Figura 11), clic en *Local*.
2. Luego clic en *Create New*.

Figura 44.- Creación de Usuario Local

3. Ingresar el nombre de usuario.
4. En caso de que se requiera mantener deshabilitada la cuenta de usuario, dar activar la opción *Disable*.
5. En *Password* ingresar la contraseña para el usuario.

   Nota: *LDAP* y *RADIUS* se habilitan en el caso de que se este creando un usuarios de Actyve Directory y Radius respectivamente.
6. Clic en *Ok*.

3.2.9.2 Grupos de Usuarios

- Los usuarios se autentican en conjunción con PPTP, L2TP, Xauth (IPSec), HTTP, FTP y TELNET.
- Los usuarios separados para diferentes servicios como IPSec (múltiples VPNs), PPTP, L2TP y HTTP.

Para agregar grupos de usuarios

1. Sobre el menú *USER* (Figura 11), Clic en *User Group*.
2. Luego clic en *Create New*.
3. Ingresar el nombre del grupo.

Figura 45.- Agregar grupos de usuarios locales

4. Seleccionar de la lista los usuarios disponibles. Usar la flecha para mover los ítems seleccionados.
5. Seleccionar el *Protection Profile* asociado al grupo donde se seleccionó la lista.
6. Clic en *OK*.

3.2.10 INTRUTION PREVENTION SYSTEM

El FortiGate Intrution Prevention System (IPS) es un sensor de detección en la red en tiempo real que usa firmas de ataques y definiciones anómalas para detectar y prevenir una amplia variedad de tráfico de red sospechoso y ataques directos basados en red.

El módulo IPS protege a la unidad FortiGate y a las redes conectadas a ésta, de ataques comunes de TCP, ICMP, UDP e IP. El IPS puede ser habilitado para prevenir un conjunto de ataques por defecto.

Para una configuración general del IPS, se necesita seleccionar cuáles interfaces deben ser monitoreadas para ataques basados en red. También se necesita decidir donde habilitar la verificación del checksum[26] que valida la integridad de los paquetes recibidos y la interfaz monitoreada.

El módulo IPS de la unidad FortiGate trabaja independiente del firewall para detectar y prevenir algunos ataques comunes.

[26] Checksum: es una forma de control de redundancia, una medida muy simple para proteger la integridad de datos, verificando que no hayan sido corrompidos.

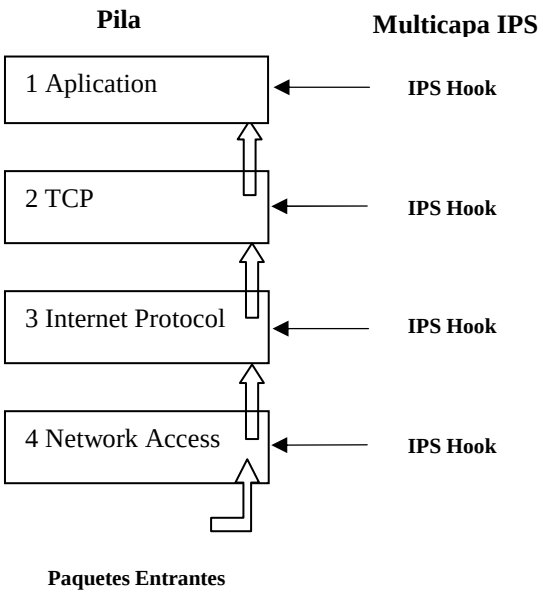


Figura 46.- El IPS puede buscar firmas de virus en todas las capas

Las firmas predefinidas de IPS y el motor IPS pueden ser actualizadas a través del FortiResponse Distribution Network. Las lista de anomalías son actualizadas con versiones del firmware.

Se puede crear firmas personalizadas en diferentes entornos de red.

Los administradores pueden ser notificados de posibles intrusiones a través de mensajes de log y alertas de e-mail.

El IPS es configurado globalmente, pero puede ser habilitado separadamente en cada protection profile.

3.2.10.1 IPS Deployment

El IPS FortiGate se ejecuta en un modo sniffer y basa su habilitación sobre una interfaz (per-interface). No puede trabajar en modo pasivo y deber ser implementado entre un firewall y la red interna.

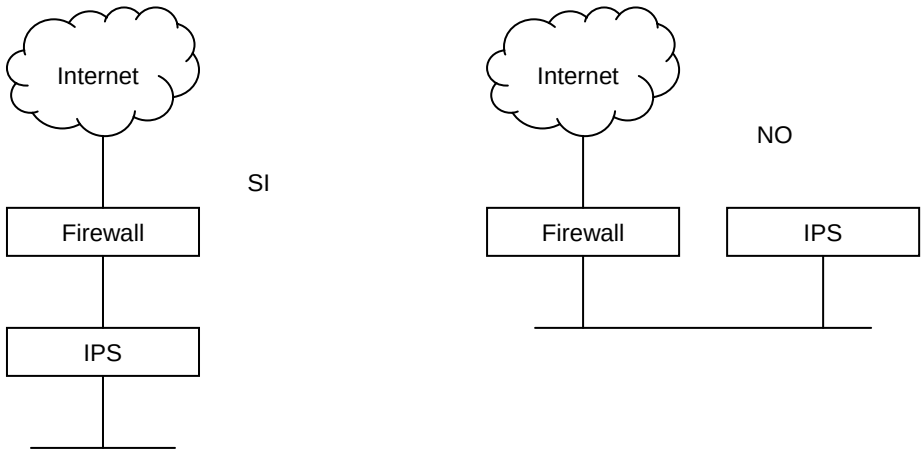


Figura 47.- IPS Deployment

Usar el IPS para:

- Redes extensas.
- Proteger redes de material altamente sensitivo.
- Redes pequeñas que requieren antivirus, filtros de spam y filtros de páginas web.

3.2.10.2 Default Settings

3.2.10.2.1 Failopen

Si por cualquier razón el IPS podría cesar de funcionar, failopen actuaría por defecto. El tráfico crucial de la red no estaría bloqueado y el firewall continuaría operando mientras el problema es resuelto. Se puede cambiar el seteo por defecto del failopen utilizando el CLI.

3.2.10.3 Configuraciones de Signature y Anomaly

Las configuraciones por defecto para Signatures y Anomalies que están implementadas por el IPS FortiGate, puede ser ajustada para acomodarse a las necesidades del tráfico. Por ejemplo, si no se está utilizando pop3, se puede deshabilitar el grupo de signature de pop3.

La mayoría de signatures están habilitadas que sólo algunas estén configuradas para pasar. Inicializar signatures para pasar por un registro de sesiones detectadas evita bloquear tráfico legítimo en la mayoría de redes.

3.2.10.4 IPS Signatures

El IPS FortiGate compara el tráfico de la red contra los patrones contenidos en una firma de ataque. Las firmas de ataque realmente protegen la red de ataques conocidos. La infraestructura del Fortinet FortiProtect asegura la rápida identificación de nuevos intentos y el desarrollo de nuevas firmas de ataque.

Las definiciones de ataque para la unidad FortiGate pueden ser actualizadas en tres maneras:

- La unidad puede ser configurada para chequear automáticamente y descargar archivos con definición de ataques actualizados.
- La unidad puede ser manualmente actualizada.
- La unidad puede ser configurada para permitir forzar actualizaciones de archivos de definición de ataques tan pronto como estos estén disponibles desde el *FortiProtect Distribution Network*.

Cuando la unidad FortiGate instala un archivo con definición de ataques actualizados, éste es revisado para ver si la configuración por defecto de cualquier firma existente ha cambiado. Si la configuración por defecto ha cambiado, los cambios son preservados.

Existen miles de firmas predefinidas en el IPS FortiGate. Adicionalmente a esta extensiva lista de firmas predefinidas de ataque, se puede crear una firma de ataque personalizada para la unidad.

Cuando un ataque ocurre, la unidad FortiGate puede registrar, pasar, abandonar, reiniciar o eliminar los paquetes sospechosos o las sesiones. Los e-mails de alerta pueden ser enviados a los administradores del sistema.

3.2.10.5 Signatures Predefinidos

Las firmas (signatures) predefinidas están arregladas dentro de grupos en base al tipo de ataque. Por defecto, todas las firmas del IPS son habilitadas. Se puede deshabilitar un grupo de signatures o un signature en particular sin pertenecer a un grupo. Deshabilitando algunos signatures puede mejorar el rendimiento del sistema y reducir el número de mensajes en el registro de IPS y mensajes de alerta que son generados. Por ejemplo, si no se provee un servidor web detrás de un firewall se podría deshabilitar todas las firmas de ataque para el servidor web.

Algunos grupos de signatures incluyen parámetros configurables. Los parámetros que están disponibles dependen del tipo de firmas en el signature group. Cuando se configuran estos parámetros para un signatures group, los parámetros se aplican a todos o a todas las firmas en el grupo. Para cada firma, se puede configurar la acción que la unidad de FortiGate toma cuando detecta un ataque. Se puede habilitar o deshabilitar la autenticación para cada ataque.

Acción	**Descripción**
Pass	El paquete que desencadenó la firma es pasado a través del firewall. Si la autenticación está deshabilitada, la acción se inicializó a *pass*, efectivamente la firma es deshabilitada.
Drop	El paquete que desencadenó la firma es abandonado. Fortinet recomienda usar una acción distinta a *drop* para conexiones basadas en ataques TCP.
Reset	El paquete que desencadenó la firma es abandonado. Una reiniciación es enviada al cliente y al servidor. La sesión es removida desde la tabla de sesiones del FortiGate. Esto es usado solamente para conexiones TCP. Si es usado para conexiones no TCP, la acción se comporta como un *Clear Session*. Si la conexión TCP está totalmente establecida previo a que se desencadene la acción de *reset*, la acción se comporta como un *Clear Session*.

Reset Client	El paquete que desencadenó la firma es abandonado. Una reiniciación es enviada al cliente. La sesión es removida desde la tabla de sesiones del FortiGate. Esto es usado solamente para conexiones TCP. Si es usado para conexiones no TCP, la acción se comporta como un *Clear Session*. Si la conexión TCP está totalmente establecida previo a que se desencadene la acción de *reset*, la acción se comporta como un *Clear Session*.
Reset Server	El paquete que desencadenó la firma es abandonado. Una reiniciación es enviada al servidor. La sesión es removida desde la tabla de sesiones del FortiGate. Esto es usado solamente para conexiones TCP. Si es usado para conexiones no TCP, la acción se comporta como un *Clear Session*. Si la conexión TCP está totalmente establecida previo a que se desencadene la acción de *reset*, la acción se comporta como un *Clear Session*.
Drop Session	El paquete que desencadenó la firma y todos los otros paquetes en la sesión son abandonados.
Clear Session	El paquete que desencadenó la firma es abandonado, la sesión es removida desde la tabla de sesiones del FortiGate y una reiniciación no es enviada.
Pass Session	El paquete que desencadenó la firma y todos los otros paquetes en la sesión son pasados a través del firewall.

Tabla 2.- Acciones del IPS FortiGate para cada firma predefinida

Para ver la lista de Firmas Predefinidas

1. Sobre el menú *IPS* (Figura 11), dar clic en *Signature*.

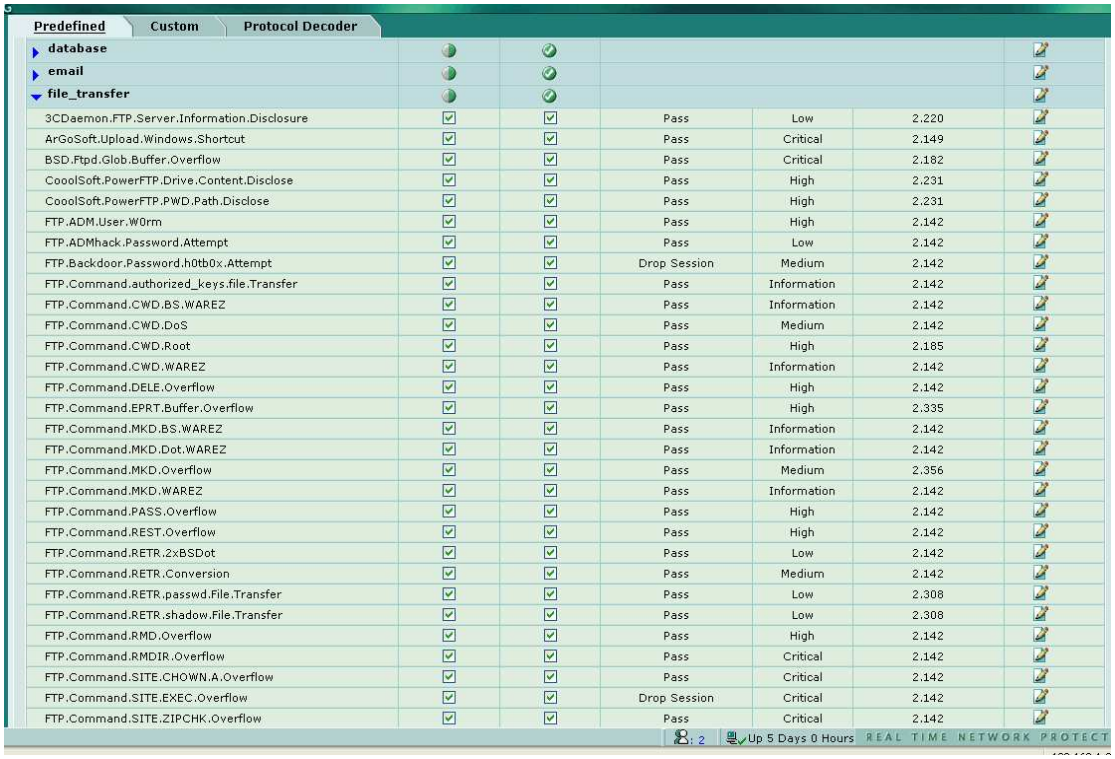


Figura 48.- Lista de Firmas (Signatures) Predefinidas del IPS

3.2.10.6 Signatures Personalizados

Proveen el poder y la flexibilidad de personalizar el IPS FortiGate para diversos entornos de red. Las firmas predefinidas cubren ataques comunes. Con firmas personalizadas, se puede proteger aplicaciones inusuales o especializadas o una plataforma no común basada sobre alertas de seguridad, revisadas por los proveedores de plataformas y aplicaciones.

3.2.10.7 Anomalies

El IPS FortiGate identifica tráfico de red que no se ajusta a patrones de tráfico conocido o pre-inicializado. El IPS FortiGate identifica los siguientes cuatro tipos de anomalías estáticas para los protocolos TCP, UDP e ICMP.

Flooding	Si el número de sesiones etiquetadas con un destino simple en un segundo supera el umbral, el destino está experimentando *flooding* (inundación).

Scan	Si el número de sesiones desde una sola fuente en un segundo sobrepasa el umbral, la fuente está experimentando *scan*.
Source	Si el número de sesiones concurrentes desde una sola fuente sobrepasa el umbral, el límite de la sesión fuente es rechazada.
Destination session limit	Si el número de sesiones concurrentes a un destino simple sobrepasa el umbral, el límite de la sesión de destino es rechazado.

Tabla 3.- Acciones del IPS FortiGate para cada anomalía predefinida

Por defecto, todas las anomalías están habilitadas. Las configuraciones individuales de anomalías pueden ser modificadas para ajustarse a las necesidades.

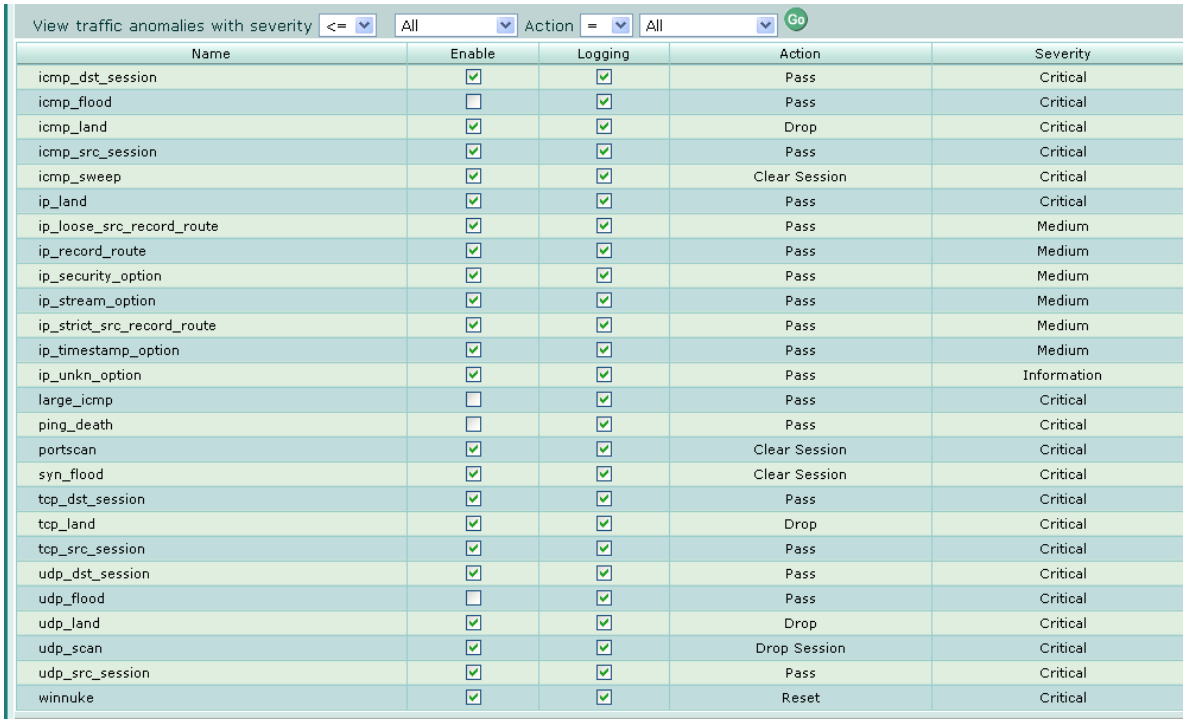


Figura 49.- Lista de Anomalies del IPS

3.2.11 SPAM FILTERING

El Spam Filtering reduce el impacto de e-mails comerciales no solicitados referentes a negocios. La pérdida de productividad, el ancho de banda desperdiciado, el proceso de correo incrementado, almacenamiento y requerimientos de archivo, serían reducidos.

El FortiGate Spam Filtering puede:

- Detener el volumen de e-mails no deseados.
- Facilitar la carga de los servidores de correo.
- Detectar spam en los e-mails recibidos.
- Prevenir transmisiones de spam desde servidores de correos remotos que son conocidos o sospechosos como distribuidores de spam.
- Etiqueta los e-mails sospechosos.
- Registra los ataques de spam.

La configuración de filtros es un sistema muy amplio, pero la implementación se basa sobre un perfil por protección. El e-mail es pasado a través de filtros en secuencia y cada filtro debe tomar acción sobre el e-mail. Si un e-mail es rechazado, la conexión entrante es abandonada inmediatamente. Después del filtrado, el estado del e-mail es revisado si éste es pasado, etiquetado o descartado.

3.2.11.1 IP Address Filtering

Los direccionamientos IP pueden ser añadidos a una lista y marcados como spam, limpiados o rechazados. Los direccionamientos IP entrantes son revisados nuevamente sobre las listas blancas y negras.

3.2.11.2 Email Address Filtering

Lo direccionamientos de e-mails pueden ser agregados a una lista y marcados como spam o limpiados. Los e-mais entrantes son revisados otra vez sobre la lista

blanca y negra. El dominio de retorno de un remitente es revisado para el intercambiador de correo (MX) o un registro A. Un registro MX crea una ruta de correo para el nombre de dominio haciendo esto posible la localización del servidor responsable para este dominio. Un registro A asigna una dirección IP al nombre de dominio.

3.2.11.3 Banned Word Filtering

Palabras y expresiones pueden agregarse a una lista y marcadas como spam o limpiadas. La cabecera, la línea de referencia, y el cuerpo del e-mail pueden ser revisados.

3.2.12 ANTIVIRUS PROTECTION

El Antivirus Protection del FortiGate 60 tiene la capacidad de realizar escaneo de virus en contenido web (http), transferencia de archivos (ftp) y correo electrónico (smtp, pop3, imap) que pasen a través del FortiGate. En el caso de que se encuentre un Virus, el Antivirus Protection remueve éste y reenvía un mensaje reemplazando la intensión del receptor.

El administrador del FortiGate puede descargar los archivos que se encuentren en cuarentena, para que sean escaneados y limpiados de virus. Además, se puede configurar para que estos archivos en cuarentena sean borrados automáticamente luego de un período de tiempo especificado.

Esta unidad también cuenta con envío de alertas de e-mails a los administradores del sistema, cuando se detecte o se remuevan virus desde el filtro de contenido.

3.2.12.1 Motor Antivirus (AV Engine)

El núcleo del motor antivirus usa firmas de virus para encontrarlos en archivos.

Un virus es encontrado si un patrón coincide con la firma de un virus que está contenido en un archivo. El núcleo del motor antivirus usa CPRL (Compact

Pattern Recognition Language) para coincidencia de patrones. El núcleo del motor antivirus primero comprueba el archivo para determinar su tipo. El motor entonces solamente busca por firmas que puedan ser de este tipo de archivo. Este rendimiento extendido se debe a que se requieren menos firmas en la coincidencia de patrones.

El tipo de archivo es determinado por la comprobación de la estructura interna del archivo. Si esto no es posible la extensión es usada como el último recurso.

3.2.12.2 Motor Heurístico

Un nuevo motor heurístico antivirus desarrolla validaciones sobre ejecutables portables (PE) archivos binarios que capturan virus que pueden ser omitidos por otros módulos de detección. Cuando las comprobaciones son completadas, los archivos pueden ser pasados, bloqueados o puestos en cuarentena.

El motor heurístico puede producir resultado de falsos positivos.

El motor heurístico es configurado usando el CLI.

3.2.13 WEB URL FILTERING Y CATEGORY BLOCK

El FortiGate Web Content Filtering puede ser configurado para escanear todo el contenido del protocolo HTTP, las tramas para URL’s y el contenido en las páginas web.

Web Filtering puede:

- Bloquear el contenido y palabras prohibidas.
- Bloquear URL’s no deseados.
- Reemplazar las páginas bloqueadas con mensajes personalizados.
- Permitir el acceso en excepciones de URL’s.
- Bloquear URL no deseado, usando las categorías del FortiGuard URL Blocking.

- Bloquear patrones URL no deseados.
- Bloquear web scripts, Java Applets, Cookies y ActiveX.

Se puede crear perfiles de protección sobre las políticas de firewall para habilitar el web filtering y category block.

3.2.13.1 Content Blocking

La unidad FortiGate puede configurarse para bloquear páginas web, si estas contienen palabras o frases prohibidas que estén añadidas en la lista del Web Banned Pattern. Estas palabras pueden ser simples o un campo de texto de hasta 80 caracteres de longitud. Cuando una página web es bloqueada es reemplazada por un mensaje que se despliega al usuario.

Para configurar Content Blocking

1. Sobre el menú *Web Filter* (Figura 11).
2. Seleccionar *Content Block*.
3. Luego clic en *Create New.*

Figura 50.- Creación de un Banned Pattern

4. Ingresar una palabra o frase:
    - Palabras - la unidad FortiGate bloquea todas las páginas web que contengan esa palabra.
    - Frases - la unidad FortiGate bloquea todas las páginas web que contengan esa frase.
    - “Frases entre comillas” - la unidad FortiGate bloquea todas las páginas web que contengan exactamente esa frase.

Nota: El máximo número de caracteres para este campo es 127.

5. Seleccionar el tipo de patrón:
   - *Wildcard*
   - *Regular Expression*
6. Seleccionar un lenguaje.
7. Seleccionar *Enable*.
8. Clic en *OK*.

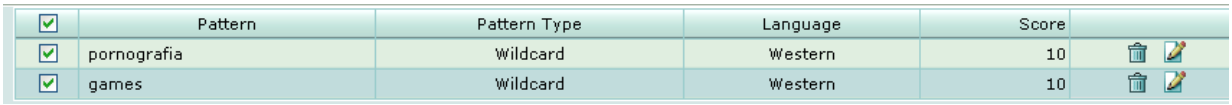


Figura 51.- Lista de Patrones creados

3.2.13.2 URL Blocking

Accesos específicos a páginas web pueden ser bloqueadas agregándolas a una lista de URL's bloqueados. Los patrones también pueden ser llenados usando texto y expresiones regulares. La unidad FortiGate bloquea cualquier página web que coincida con los URL's o patrones especificados, y despliega un mensaje al usuario.

Para configurar URL Blocking

1. Sobre el menú *Web Filter* (Figura 11), seleccionar *URL Filter*.
2. Luego, dar clic en *Create New*.
3. Ingresar un URL:
   - Un URL completo para bloquear el acceso a todas las páginas de un sitio web. (www.badsite.com).
   - Una dirección IP para bloquear el acceso a todas las páginas de un sitio web (200.107.43.100).
   - Un URL parcial para bloquear sub-dominios (nasty.com)
   - Un sufijo de dominio para bloquear todos los URL's que contengan ese sufijo (com).

Figura 52.- Creación de URL Filter

Nota: No se debe incluir http:// en el URL.

4. Seleccionar *Enable*.
5. Clic en *OK*.

Figura 53.- Lista de URL Filter creados

3.2.13.3 URL Exempt List

Legitima URL's que pueden ser bloqueados por el contenido o bloquear URL's que pueden ser añadidos a una lista de exentos.

Para configurar URL Exempt List

1. Sobre el menú *Web Filter* (Figura 11), seleccionar *URL Exempt.*
2. Luego, dar clic en *Create New*.

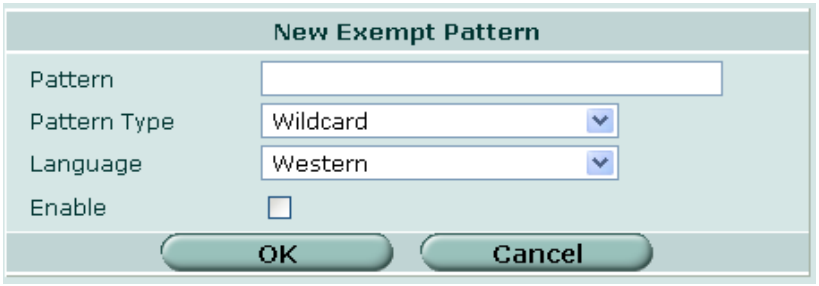


Figura 54.- Creación de URL Exempt

3. En Pattern, ingresar una palabra o frase:

- Palabras - la unidad FortiGate bloquea todas las páginas web que contengan esa palabra.
- Frases - la unidad FortiGate bloquea todas las páginas web que contengan esa frase.
- “Frases entre comillas” - la unidad FortiGate bloquea todas las páginas web que contengan exactamente esa frase.

4. Seleccionar el tipo de patrón:
    - *Wildcard*
    - *Regular Expression*
5. Seleccionar un lenguaje.
6. Seleccionar *Enable*.
7. Clic en *OK*.

3.2.14 FORTIGUARD

FortiGuard:

- Es un administrador de soluciones web filtering.
- Clasifica cientos de millones de páginas web en un rango extenso de categorías.
- Puede permitir, bloquear o monitorear páginas web.
- Tiene una cobertura extensa para todo el mundo, provista por FortiGuard Service Point.
    - La unidad FortiGate se comunica con el Service Point más cercano.
    - Los nuevos puntos son agregados como requeridos.
- Es escalable

Los usuarios pueden hospedar su propio FortiGuard Service Point.

El siguiente diagrama muestra la topología FortiGuard:

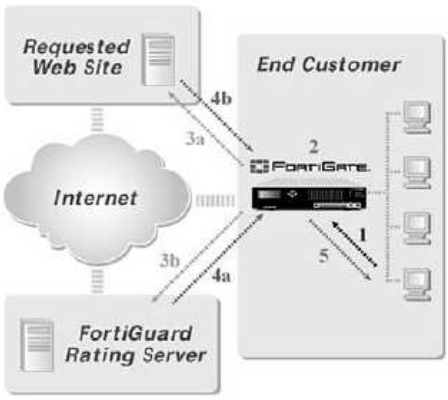


Figura 55.- Topología FortiGuard

Para habilitar Fortiguard

1. Sobre el menú *System* (Figura 11), clic en *Maintenance*.
2. Ir a la pestaña *FortiGuard Center*.

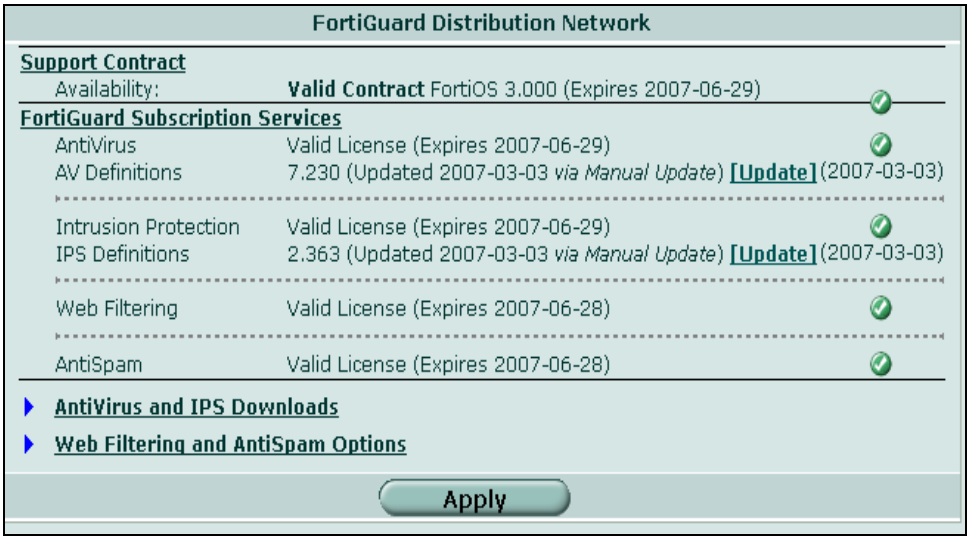


Figura 56.- FortiGuard Distribution Network

3. Seleccionar *Enable Service*.
4. Seleccionar *Check Status* para asegurase que la unidad FortiGate puede acceder al servidor FortiGuard. El estado del FortiGuard debería cambiar de *Unknow* a *Available*. Si el estado del FortiGuard es *unavailable*, esperar e intentar nuevamente.
5. Si se desea, habilitar y setear un *TTL* (time to live).

6. Clic en *Apply*.

Ahora se puede habilitar *Web Category Blocking* y configurar categorías para cualquier protection profile creados en el firewall.

3.2.14.1 Configurando FortiGuard

Se puede:

- Configurar las opciones de Web Category Filtering para los protection profile.
- Permitir, bloquear, o monitorear categorías o grupos de categorías.
- Aplicar diferentes opciones de Web Category Filtering a protection profile para diferentes grupos de usuarios como sean requeridos.

Para crear perfiles de protección que use Web Category Filtering:

1. Sobre el menú *Firewall* (Figura 11), clic en *Protection Profile*.
2. Clic en *Create New*.
3. Ingresar un nombre para el *Protection Profile*.
4. Expandir la lista de opciones del *Web Category Filtering*.

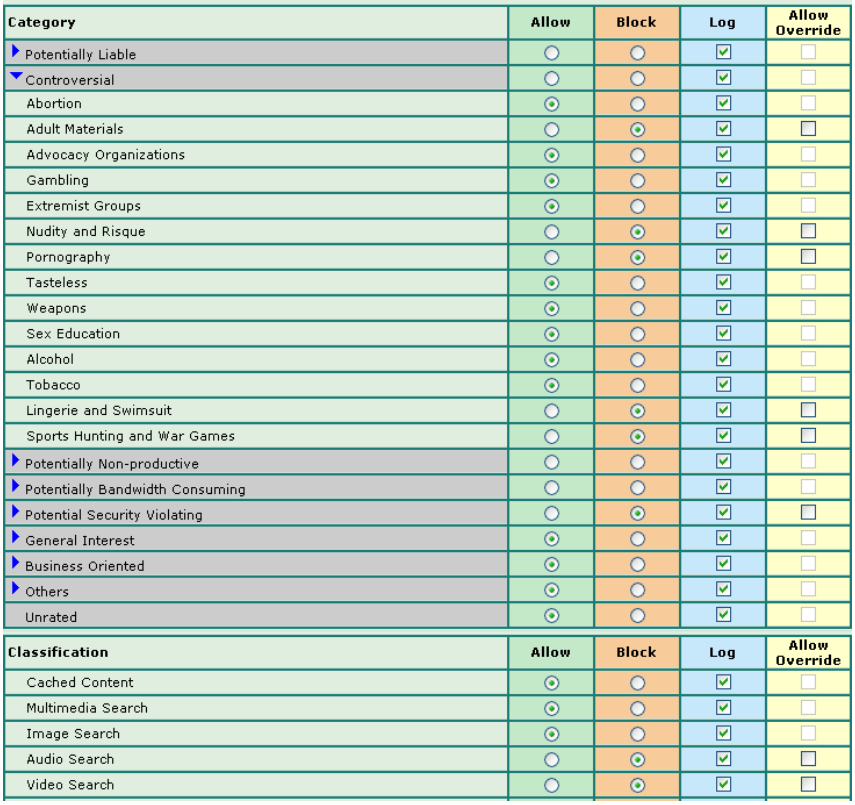


Figura 57.- Categorías FortiGuard Web Filtering

5. Seleccionar *Enable Category Block*.
6. Expandir las categorías o grupos de categorías del FortiGuard Web Filtering y seleccionar *Allow* (permitir), *Block* (bloquear) o *Monito*r (monitorear).
7. Configurar cualquier otra opción requerida en el Protecction Profile.
8. Clic en *OK*.

Ahora se puede agregar el Protection Profile a cualquier política de firewall. El Protection Profile también puede ser agregado a grupos de usuarios y estos ser usados para aplicar autenticación a las políticas de Firewall.

3.2.14.2 Agregar Protection Profiles a políticas de Firewall

Añadiendo un Protecction Profile a una política de Firewall aplicando las configuraciones del perfil, incluyendo web Category Filtering al tráfico que coincide con la política.

3.2.14.3 Agregar Protection Profiles a grupos de usuarios

Cuando se crea grupos de usuarios se puede también seleccionar un Protection Profile que aplica al grupo. Entonces, cuando se configura una política de firewall que incluiye la autenticación de usuario, se selecciona uno o más grupos de usuario para autenticar. Cada grupo de usuario que se selecciona para autenticación en la política de firewall puede tener un Protection Profile diferente, y a pesar de eso diferentes configuraciones en el FortiGuard Web Filtering, aplicadas a este.

3.2.15 REGISTRO DEL EQUIPO

Para registrar la unidad FortiGate 60 de Fortinet, es necesario ingresar a la página web https://support.fortinet.com, dentro de ésta ingresar en la opción *Product Registration*, (Figura 58).

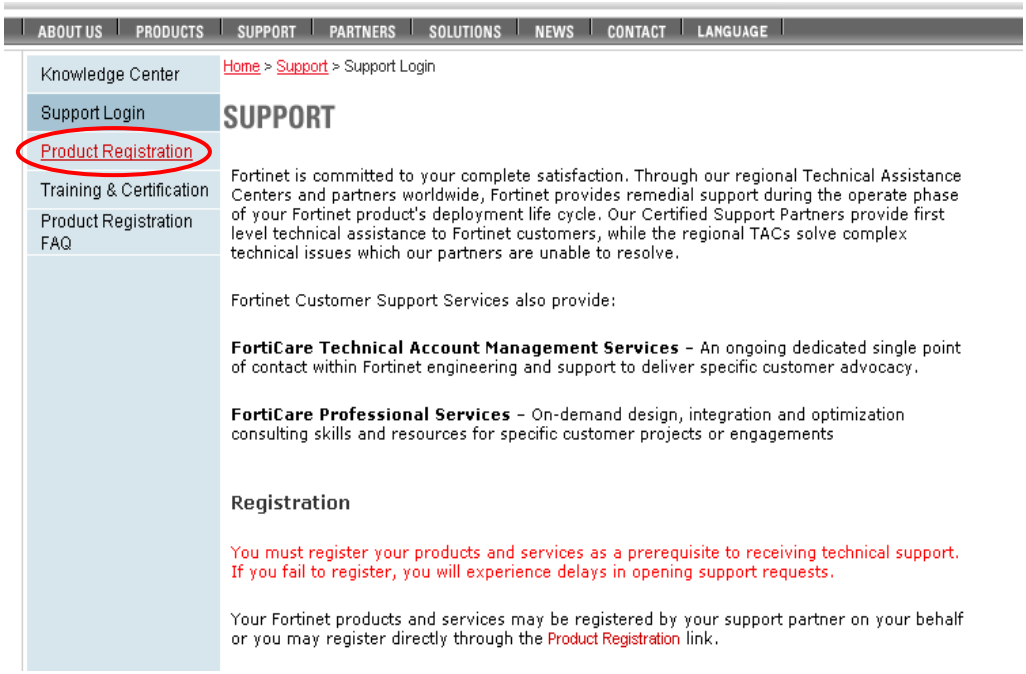


Figura 58.- Página Web de Soporte de Fortines

Ingresar todos los datos requeridos para registrar un contacto del equipo Fortinet, y luego dar clic en *Next*, (Figura 59).

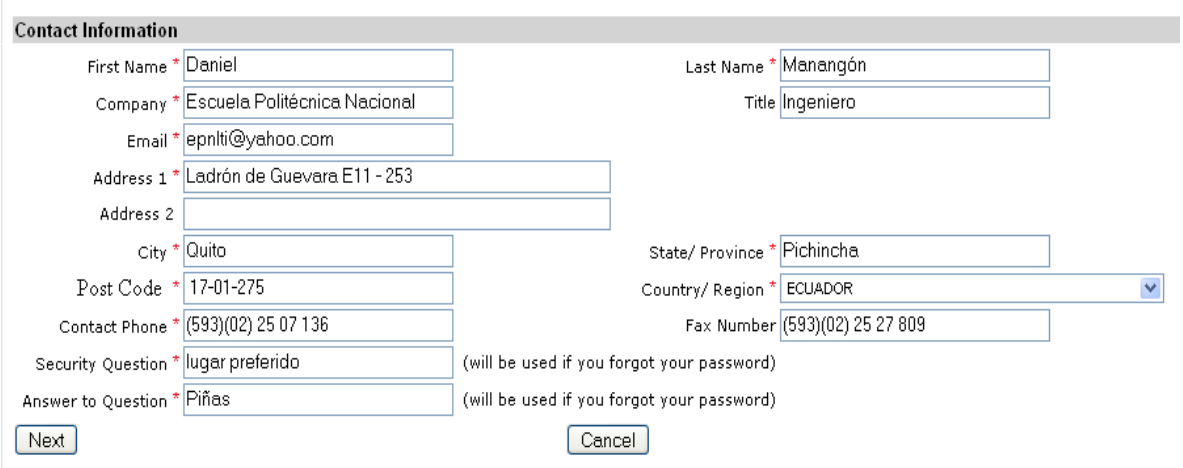


Figura 59.- Registro del firewall FortiGate 60 en Fortinet

Una vez enviada la información, se recibirá un correo electrónico a la dirección del contacto ingresado, en este caso a: epnlti@yahoo.com. En el cuál consta la confirmación del registro del equipo y el nombre de usuario y contraseña para ingresar a la página de soporte de Fortinet.

3.2.16 ADMINISTRACIÓN Y MANTENIMIENTO

3.2.16.1 Actualizaciones Automáticas

Se puede configurar la unidad FortiGate 60 para conectarse al *FortiResponse Distribution Network (FDN)* para actualizaciones de antivirus y definiciones de ataques y motores de antivirus el FDN es una red amplia global de *FortiResponse Distribution Servers (FDSs)*. Cuando la unidad FortiGate se conecta a la FDN, éste se conecta al FDS más cercano. Al hacer esto, todas las unidades de FortiGate están programadas con una lista de direcciones FDS clasificadas por el más cercano, acorde a la zona horaria configurada en la unidad FortiGate.

Los siguientes elementos de actualización están disponibles:

- User-initiated actualizados desde el FDN.
- Schedules actualizados de la última versión cada hora, día o semana desde el FDN.
- Empujar actualizaciones iniciadas por el FDN cuando una nueva actualización está disponible.

- El estado de la actualización incluye número de versión, fechas de expedición y actualización de fechas y horas.
- Empujar actualizaciones a través de un dispositivo NAT.

Para recibir actualizaciones programadas, se debe registrar la unidad FortiGate, en la página web de soporte del Fortinet.

Para configurar actualizaciones automáticas

1. Sobre el menú *System* (Figura 11), clic en *Maintenance*.
2. Luego, ir a la pestaña *FortiGuard Center*,

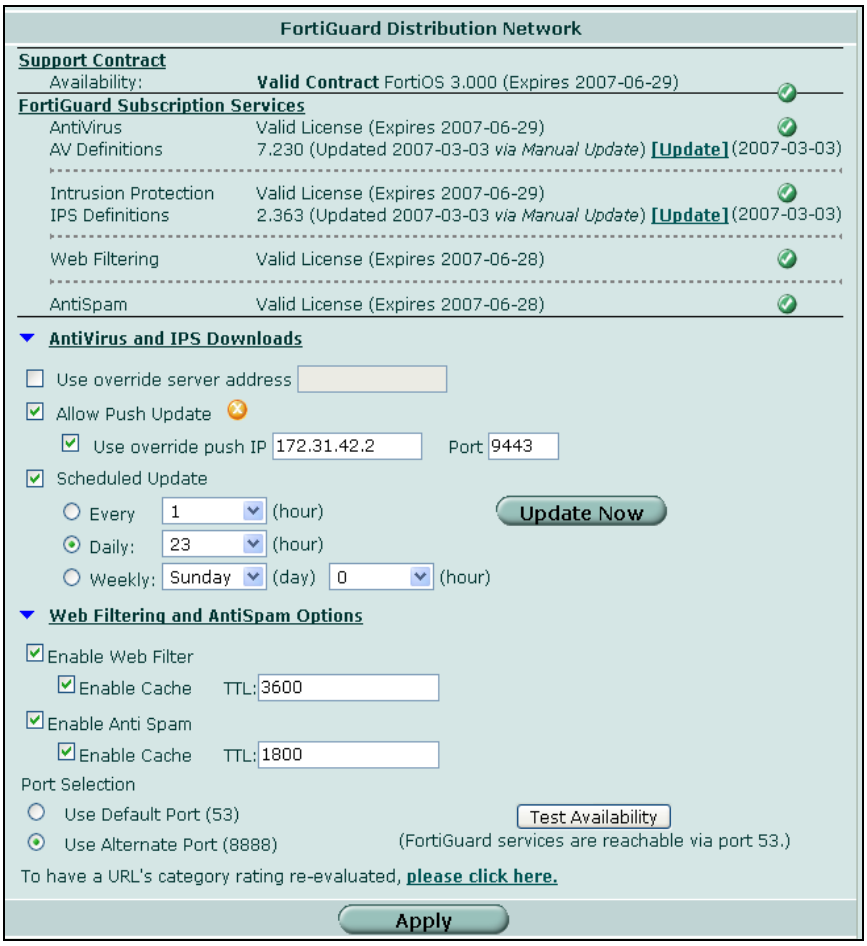


Figura 60.- Configuración de actualizaciones automáticas de definiciones de IPS y Antivirus

3. Habilitar la opción *Allow Push Update* (Figura 60).
4. Seleccionar *Use override push IP*, e ingresar la dirección.

5. Seleccionar *Schedule Update*, y elegir una de las siguientes opciones:
   - Every: una vez de cada 1 a 23 horas. Seleccionar el número de horas entre cada actualización.
   - Daily: una vez al día, especificando la hora del día para que cheque las actualizaciones.
   - Weekly: una vez a la semana. Especificar el día de la semana y la hora del día para revisar las actualizaciones
6. Clic en *Apply*.

3.2.16.2 Actualización de Firmware

Nota: La instalación del Firmware reemplaza las actuales definiciones de antivirus y ataques con las definiciones incluidas en la revisión del firmware que se está instalando.

Para Actualizar el Firmware

1. Copiar el archivo imagen del firmware a un computador
2. Ingresar al modulo de administración basado en web, con permisos de administrador.
3. Sobre el menú *System*, clic en *Status*.

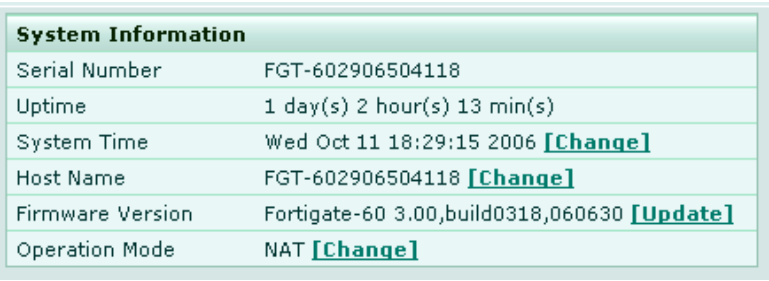


Figura 61.- Información del Sistema

4. Dar clic en *Update*, bajo la unidad de información *Firmware Version*.
5. Buscar la ubicación del archivo procesado en el paso 1.
6. Clic en *OK*.

La unidad FortiGate 60 carga el archivo imagen del firmware, actualiza esta nueva versión, se reinicia y despliega la ventana de inicio del FotiGate. Este proceso toma unos pocos minutos.

7. Ingresar nuevamente a la administración basada en web.
8. En el menú *System* dar clic en *Status* para revisar la versión de Firmware y confirmar que la actualización se instaló satisfactoriamente.

3.2.16.3 Backups

La unidad FortiGate 60 cuenta con la opción de respaldar su configuración en cualquier momento que se requiera.

Para realizar Backup del sistema

1. Sobre el menú *System* (Figura 11), clic en *Maintenance*.
2. Luego ubicarse en la pestaña *Backup & Restore*.

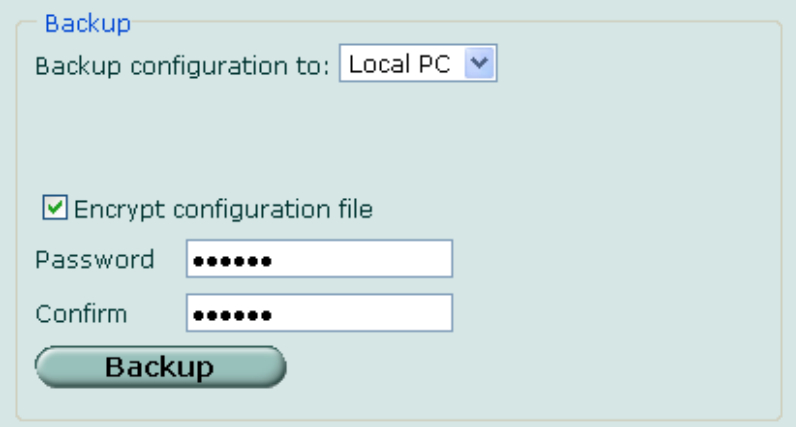


Figura 62.- Backup de la configuración del equipo

3. Si se de desea habilitar la opción *Encrypt configuration file*, para encriptar la información a través de una contraseña.
4. Dar clic en *Backup*.
5. Escoger una ubicación, en cualquier disco de almacenamiento, donde se guardará el archivo y editar un nombre para el mismo. Luego clic en *Guardar*.

3.2.16.4 Restore

La unidad FortiGate 60 también cuenta con la opción de restaurar la configuración respaldad. Para esto seguir los siguientes pasos:

Para realizar Restore del sistema

1. Sobre el menú *System* (Figura 11), clic en *Maintenance*.
2. Luego ubicarse en la pestaña *Backup & Restore*.
3. Dar clic en *Examinar* para ubicar el archivo de configuración.

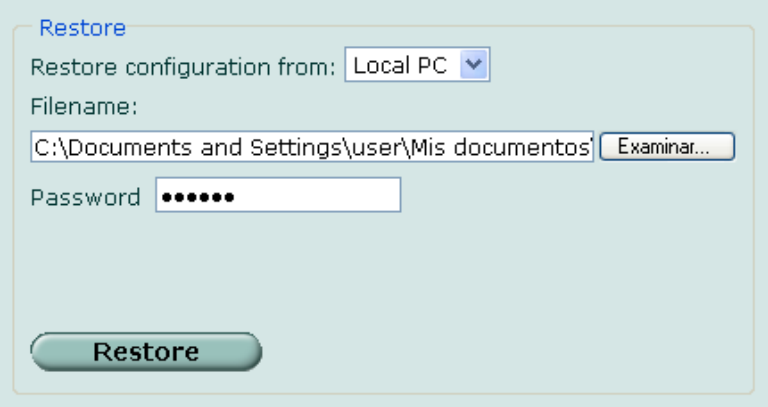


Figura 63.- Restauración de la configuración del equipo

4. En el caso de haber encriptado el archivo, ingresar en el campo *Password* la contraseña correspondiente.
5. Dar clic en *Restore*. El proceso puede tomar unos minutos.

3.2.16.4 Usuarios Administradores

Es posible crear más de una cuenta de usuario administrador para ingresar a la configuración del sistema.

Para crear un usuario administrador

1. Sobre el menú *System* (Figura 11), clic en *Admin*.
2. Sobre la pestaña *Administrators*, clic en *Create New*.

Figura 64.- Creación de un usuario Administrador

3. En el campo *Administrador*, ingresar un nombre de usuario (Figura 64).
4. En el campo *Password*, ingresar una contraseña para el usuario adminstrador.
5. En el campo *Confirm Password*, ingresar la contraseña para el usuario administrador por segunda vez, para confirmar que esté correcta.
6. En los campos *Trusted Host*, si se desea se puede ingresar la dirección IP de un equipo con su respectiva máscara de subred, para que el acceso como administrador a la unidad FortiGate sea restringido. Se puede especificar hasta tres Trusted Host.
7. En el campo *Access Profile*, seleccionar el perfil de acceso para el administrador. El perfil pre-configurado *prof_admin* provee acceso total a la unidad FortiGate. Se puede también seleccionar *Create New* para crear un nuevo perfil de acceso.
8. Clic en *Ok*.

Para crear un Perfil de Acceso

1. Sobre el menú *System* (Figura 11), clic en *Admin*.
2. Ir a la pestaña *Access Profile*, clic en *Create New*.

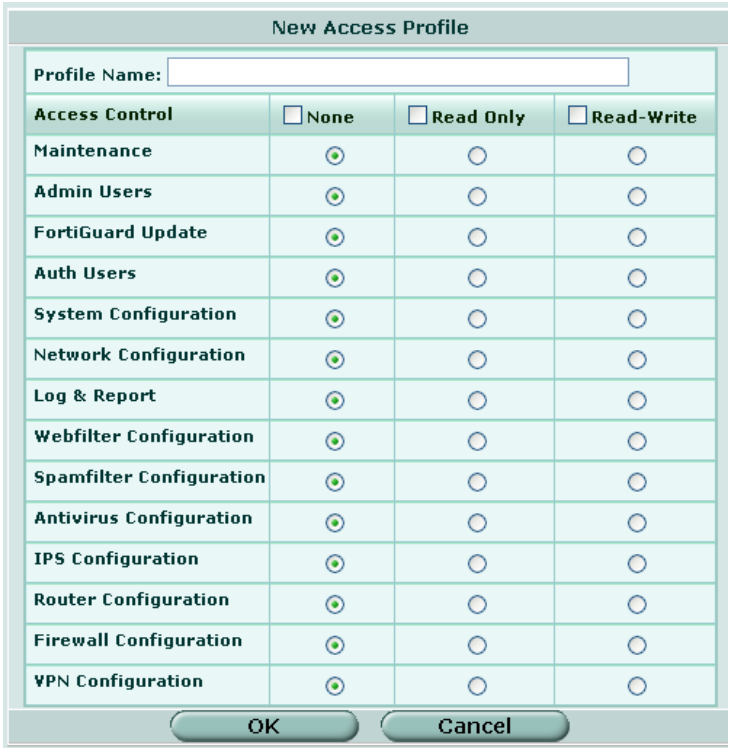


Figura 65.- Creación de un Perfil de Acceso

3. En el campo *Profile Name* ingresar el nombre del perfil de acceso (Figura 65).
4. En *Access Control* se listan las opciones de control de acceso del perfil que se va a crear.
5. Si se desea habilitar *Read Only*, para seleccionar acceso de solo lectura en todas las categorías de control de acceso.
6. Si se desea habilitar *Read Write*, para seleccionar acceso de lectura y escritura en todas las categorías de control de acceso.
7. También se puede seleccionar *Read* y/o *Write* por categorías del control de acceso como se requiera
8. Clic en *Ok*.

Para cambiar la clave de usuario administrador

1. Sobre el menú *System* (Figura 11), clic en *Admin*.
2. Ir a la pestaña *Administrators*.

3. Sobre el usuario dar clic en *Change Password*. En este caso el usuario es *admin*.

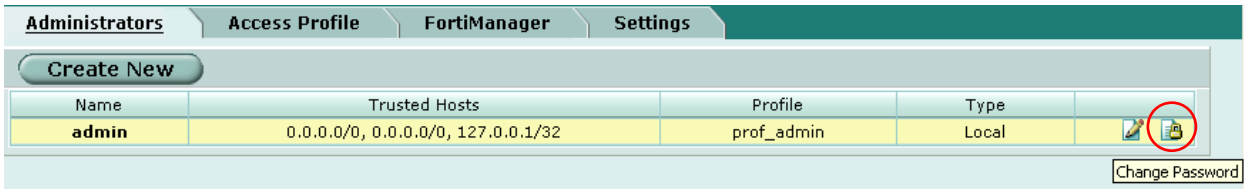


Figura 66.- Lista de usuarios administradores creados

4. En el campo *Old Password*, ingresar la clave actual.
5. En el campo *New Password*, ingresar la nueva clave.
6. En el campo *Confirm Password*, confirmar la nueva clave.

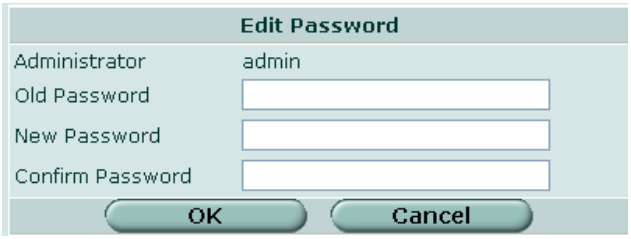


Figura 67.- Cambio de la clave de un usuario administrador

7. Clic en *Ok*.

3.2.16.5 Ajustes de Administración

La unidad FortiGate 60 permite configurar o personalizar los puertos para HTTP y HTTPS para el acceso administrativo. Los tiempos de interrupción, que incluye la interrupción de tiempo no útil y la interrupción de autenticación, además el lenguaje de la interfaz de administración basada en Web.

Para cambiar los Ajustes de Administración

1. Sobre el menú *System* (Figura 11), clic en *Admin*.
2. Ir a la pestaña *Settings*.

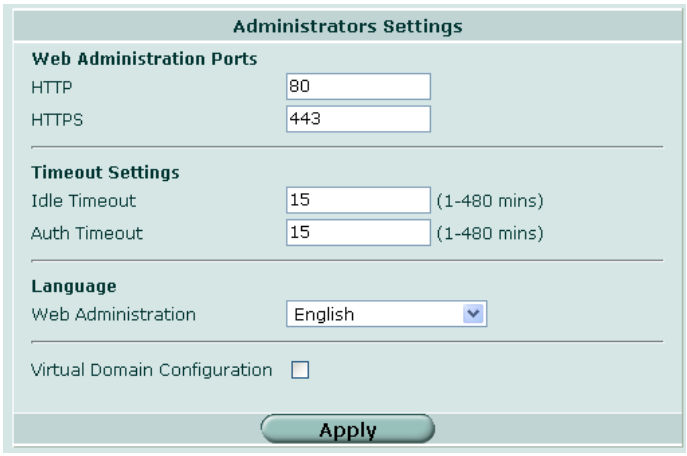


Figura 68.- Configuraciones de Administración

3. Si se desea, cambiar el puerto TCP para el acceso administrativo HTTP. O mantener el puerto por defecto que es el puerto 80.
4. Si se desea, cambiar el puerto TCP para el acceso administrativo HTTPS. O mantener el puerto por defecto que es el puerto 443.
5. En *Idle Timeout*, ingresar el número de minutos en que la conexión administrativa pueda estar en inacción, antes de que el administrador haga login nuevamente.
6. En *Auth Timeout*, ingresar el número de minutos en que la conexión autenticada pueda estar en inacción, antes de que el usuario pueda autenticarse nuevamente.
7. En *Language*, escoger el idioma para usar la interfaz de administración basada en web.
8. Habilitar *Virtual Domain Configuration*, si se desea operar con múltiples dominios virtuales.

3.3 RESUMEN TÉCNICO GENERAL DEL SISTEMA DE SEGURIDAD

La red del LTI está constituida por una conexión directa de Internet proporcionada por la UGI, la misma que se conecta a un switch de capa 2, a éste se encuentra enlazado la unidad FortiGate a través de la interfaz wan1. Adicionalmente este firewall presenta tres interfaces de configuración, wan2, dmz, internal (Figura 69).

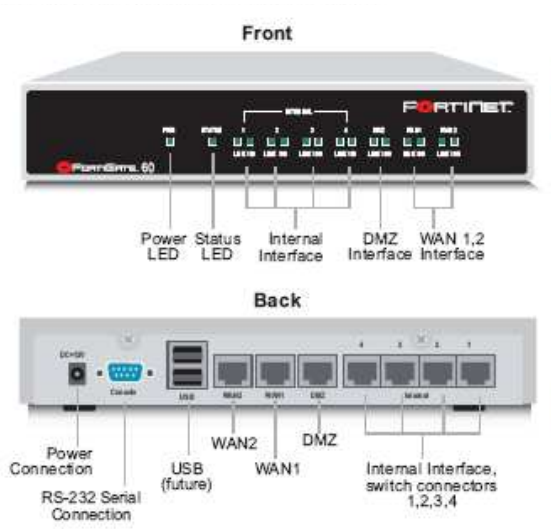


Figura 69 .- Interfaces de la unidad FortiGate 60

El LTI dispone de un servidor Web que tiene una entrada de red pública. La misma que tiene asignada una dirección IP estática por la UGI, destinada para el uso del servicio Web. Este servidor está fuera del alcance de protección del firewall porque fue implementado después del desarrollo del sistema de seguridad de la red.

Esquema de configuración del Firewall

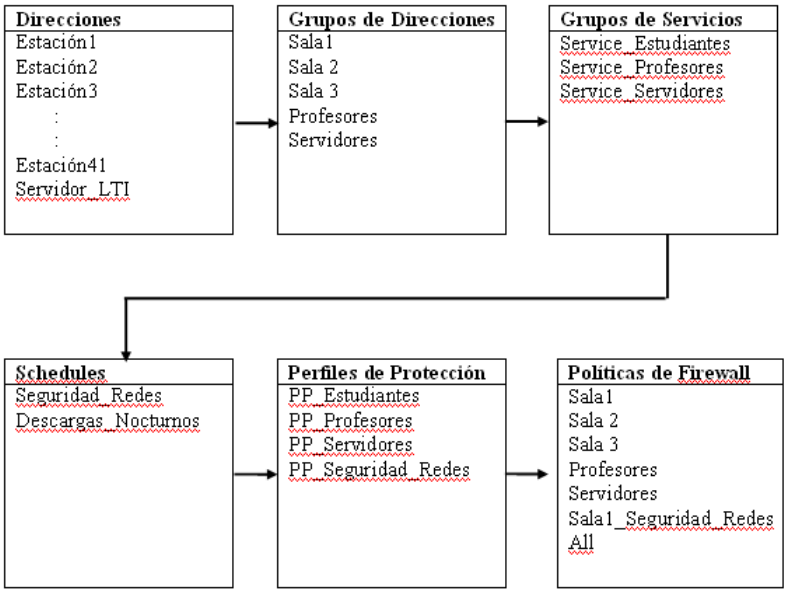


Figura 70 .- Esquema de Configuración del Firewall

En la interfaz internal se encuentra configurada la subred LAN del laboratorio. En esta interfaz está habilitado el DHCP del FortiGate, el mismo que se encarga de asignar direcciones IP dinámicas a cada estación de trabajo y además permite que el tiempo de asignación de estas direcciones sea ilimitado, es decir que se mantenga siempre la dirección IP asignada a dicha estación.

Cada estación de trabajo está registrada en la unidad FortiGate 60 con su respectiva dirección IP asignada, para identificarla dentro del equipo. Y a la vez éstas están incluidas en grupos de direcciones para facilitar el control y la administración de la red.

De acuerdo a las necesidades de cada grupo de direcciones, está asignado un perfil de protección, el mismo que se encarga de proveer Antivirus, Web Filtering, FortiGuard Web Filtering, Spam Filtering.

Estos perfiles de protección están relacionados con las políticas de firewall, las mismas que, según su configuración, se encargan permitir o denegar la conexión

según las peticiones de cada usuario. Con el objetivo de proteger la red desde la interfaz interna hacia la externa (wan 1).

El firewall FortiGate 60 tiene una consola de administración basada en web muy amigable e intuitiva para el administrador de la red, que facilita su configuración y administración.

CAPITULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

El perímetro de seguridad que ofrece la unidad FortiGate es extensa porque tiene la capacidad de soportar hasta 2000 sesiones concurrentes (sc), y se ha comprobado que en horas donde el laboratorio registra el mayor número de usuarios conectados a Internet, puede generar un máximo de 900 sc, quedando así demostrado que la red LTI tiene un margen amplio de capacidad de un crecimiento planificado o permitido.

Nota: El modelo de FortiGate 60 que fue liberado por el fabricante como un equipo de entrenamiento, no dispone de todos los elementos o capacidades para tenerlo todo el tiempo en uso.

La unidad FortiGate ha permitido a los usuarios la obtención de información segura a través de categorización de páginas que puedan ser accedidas, así como también realizar descargas de sitios seguros.

A través del sistema de seguridad implementado en el LTI, se ha conseguido que la Unidad de Gestión de Información (UGI) de la Escuela Politécnica Nacional, obtenga mejores resultados en cuanto a la saturación del ancho de banda.

4.2 RECOMENDACIONES

Se recomienda la renovación del licenciamiento de la unidad FortiGate 60, en vista de que necesita del mismo para su óptimo funcionamiento.

Se recomienda, también habilitar la interfaz DMZ para obtener una mayor protección y control de los servidores, para salvaguardar la integridad de los mismos.

Es importante que la unidad FortiGate mantenga actualizadas las definiciones de ataques y antivirus para evitar que cualquier amenaza de virus o intrusos se propaguen a través de la red.

Se recomienda NO habilitar la autenticación de usuarios en las políticas de firewall configuradas para permitir el paso de servicios, ya que el uso del laboratorio es por múltiples usuarios y para múltiples tareas. Por lo que resulta más fácil controlar el tráfico por cada estación de trabajo a hacerlo por cada usuario.

Para mayor seguridad, se recomienda revisar con frecuencia que las direcciones IP asignadas en cada estación de trabajo coincidan con las direcciones IP ingresadas en la unidad FortiGate 60.

Se recomienda generar un archivo de respaldo, cada vez que se realicen cambios en la configuración del firewall. Para en caso de cualquier fallo del sistema poder restaurar la última configuración del equipo.

Se recomienda hacer un monitoreo de sesiones concurrentes, para determinar el tráfico generado por cada una de las estaciones de trabajo; y relacionar los resultados obtenidos, con el número de sesiones permitidas por el fabricante.

Se recomienda que el personal responsable del mantenimiento y administración de la red del LTI, mediante consenso, definan las políticas de firewall a implementarse según las necesidades del día a día.

Para lograr una mayor optimización en la transmisión de datos, se recomienda implementar el enlace LTI – UGI con fibra óptica, ya que facilitaría el intercambio de información y prestaría mayor seguridad a la misma.

GLOSARIO

Adware.- Son aquellos programas que muestran publicidad utilizando cualquier tipo de medio, por ejemplo: ventanas emergentes, banners, cambios en la página de inicio o de búsqueda del navegador, etc.

Antivirus.- Brinda protección contra los archivos que entran a la red a través del correo electrónico, descargas de Internet, discos extraíbles, etc.

Banner.- Es un anuncio mostrado en una página web, sobre un determinado producto o servicio propio o ajeno a la página y que, al ser pulsado, lleva al sitio del anunciante.

Checksum.- Una suma de verificación o checksum es una forma de control de redundancia, una medida muy simple para proteger la integridad de datos, verificando que no hayan sido corrompidos.

Cracker.- Es una persona interesada en saltarse la seguridad de un sistema informático.

Dialer: Es un programa que suele ser utilizado para redirigir, de forma maliciosa, las conexiones mientras se navega por Internet. Su objetivo es colgar la conexión telefónica que se está utilizando en ese momento y establecer otra, marcando un número de teléfono de tarificación especial. Esto supondrá un notable aumento del importe en la factura telefónica.

DHCP.- Dynamic Host Configuration Protocol, es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente.

DMZ.- La arquitectura Screened Subnet, también conocida como red perimétrica o De-Militarized Zone (DMZ), añade un nivel de seguridad en las arquitecturas de

cortafuegos situando una subred (DMZ) entre las redes externa e interna, de forma que se consiguen reducir los efectos de un ataque exitoso al host bastión.

DNS.- Domain Name System o Sistema de Nombres de Dominio, es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet.

Eavesdropping.- La interceptación o eavesdropping, también conocida por passive wiretapping es un proceso mediante el cual un agente capta información - en claro o cifrada - que no le iba dirigida; esta captación puede realizarse por muchísimos medios.

Firewall.- También llamado cortafuegos, es un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que se hayan definido en la red.

Firmware.- es un bloque de instrucciones de programa para propósitos específicos, grabado en una memoria tipo ROM, que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo.

FTP.- File Transfer Protocol, es un protocolo de transferencia de archivos entre sistemas conectados a una red TCP basado en la arquitectura cliente-servidor, de manera que desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle sus propios archivos independientemente del sistema operativo utilizado en cada equipo. El Servicio FTP es ofrecido por la capa de Aplicación del modelo de capas de red TCP/IP al usuario, utilizando normalmente el puerto de red 20 y el 21.

HTTP.- El protocolo de transferencia de hipertexto es usado en cada transacción de la Web (WWW). El hipertexto es el contenido de las páginas web, y el

protocolo de transferencia es el sistema mediante el cual se envían las peticiones de acceso a una página y la respuesta con el contenido.

HTTPS.- Es la versión segura del protocolo HTTP. El sistema HTTPS utiliza un cifrado basado en las Secure Socket Layers (SSL) para crear un canal cifrado (cuyo nivel de cifrado depende del servidor remoto y del navegador utilizado por el cliente) más apropiado para el tráfico de información sensible que el protocolo HTTP. Cabe mencionar que el uso del protocolo HTTPS no impide que se pueda utilizar HTTP. El puerto estándar para este protocolo es el 443.

ICMP.- Internet Control Message Protocol o Protocolo de Control de Mensajes de Internet, es el sub-protocolo de diagnóstico y notificación de errores del Protocolo de Internet (IP).

IDS.- Intrution Detection System o Sistema de Detección de Intrusiones, es una herramienta de seguridad que intenta detectar o monitorizar los eventos ocurridos en un determinado sistema informático o red informática en busca de intentos de complicar la seguridad de dicho sistema.

IP.- Internet Protocol o Protocolo Internet, es un protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados.

IPS.- Intrution Prevention System o Sistema de Prevención de Intrusos, es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

Kerberos.- Es un protocolo de autenticación de redes de computador que permite a dos computadores en una red insegura demostrar su identidad mutuamente de manera segura.

LDAP.- Lightweight Directory Access Protocol es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido

para buscar diversa información en un entorno de red. LDAP puede considerarse una base de datos (aunque su sistema de almacenamiento puede ser diferente) al que pueden realizarse consultas.

Malware.- es software que tiene como objetivo infiltrarse en o dañar un computador sin el consentimiento informado de su dueño. Existen muchísimos tipos de malware, aunque algunos de los más comunes son los virus informáticos, los gusanos, los troyanos, los programas de spyware/adware o incluso los bots.

MTU.- La unidad máxima de transferencia (Maximum Transfer Unit) es un término de redes de computadoras que expresa el tamaño en bytes del datagrama más grande que puede pasar por una capa de un protocolo de comunicaciones. Los datagramas pueden pasar por varios tipos de redes con diferentes protocolos antes de llegar a su destino. Por tanto, para que un datagrama llegue sin fragmentación al destino, ha de ser menor o igual que el mínimo MTU de las redes por las que pase. Ejemplos de MTU: Ethernet: 1500 bytes. ATM (AAL5): 8190 bytes. FDDI: 4470 bytes. PPP: 576 bytes.

Pattern Type.- es el tipo de extensión de un archivo, por ejemplo *.exe, *.com, *,bat, *.zip. Esto sirve para bloquear con el menú antivirus, para bloquear la descargar esos tipos de pattern type.

Perfil de Protección.- Un perfil de protección (Protection Profile) define un conjunto de objetivos y requisitos de seguridad, independiente de la implantación, para una categoría de productos que cubre las necesidades de seguridad comunes a varios usuarios. Los perfiles de protección son reutilizables y normalmente públicos.

Phishing: El phishing consiste en el envío masivo de mensajes que, aparentando provenir de fuentes fiables, intentan conseguir que el usuario proporcione datos confidenciales. El caso más típico de phishing es el envío de correos electrónicos que se hacen pasar por procedentes de una entidad bancaria online, para conseguir que el usuario introduzca sus contraseñas en una página web falseada.

Política de Firewall.- La función política de firewall permite ver y modificar las configuraciones de firewall (reglas de acceso y reglas de inspección) en el contexto de las interfaces cuyo tráfico filtran.

RADIUS.- El Servicio de usuario de acceso telefónico de autenticación remota (RADIUS, Remote Authentication Dial-In User Service) se utiliza para proporcionar servicios de autenticación, autorización y administración de cuentas. Un cliente RADIUS envía credenciales de usuario e información de parámetros de conexión en forma de un mensaje RADIUS a un servidor RADIUS. El servidor RADIUS autentica y autoriza la petición del cliente RADIUS y devuelve un mensaje de respuesta RADIUS.

Regular expresión.- sirve para bloquear el contenido de páginas web según la palabra o expresión ingresada en este campo.

Signature.- Estas firmas reflejan patrones en la actividad del sistema o de la red que señalan un posible ataque de virus o pirata informático. Los sistemas de detección de intrusión y cortafuegos (firewalls) utilizan estas firmas para distinguir entre actividad legítima y potencialmente maliciosa.

SNMP.- Simple Network Management Protocol o Protocolo Simple de Administración de red, es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. SNMP permite a los administradores supervisar el desempeño de la red, buscar y resolver sus problemas, y planear su crecimiento.

Spam: Es correo electrónico no solicitado, normalmente con contenido publicitario, que se envía de forma masiva. Este tipo de mensajes pueden causar graves molestias y provocar pérdidas de tiempo y recursos.

Spyware.- Son aquellos programas que recopilan datos sobre los hábitos de

navegación, preferencias y gustos del usuario. Dichos datos son transmitidos a los propios fabricantes o a terceros, cabiendo la posibilidad de que sean almacenados de alguna manera para ser posteriormente recuperados.

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 el computador mediante un intérprete de comandos.

Subrepticio.- Esto significa que el virus informático utilizará varias técnicas para evitar que el usuario se de cuenta de su presencia.

TCP.- Transmission Control Protocol o Protocolo de Control de Transmisión, este protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. Las conexiones TCP se componen de tres etapas: establecimiento de conexión, transferencia de datos y fin de la conexión.

Telnet.- sirve para acceder mediante una red a otra máquina, para manejarla como si se estuviera dentro de ella. Para que la conexión funcione, como en todos los servicios de Internet, la máquina a la que se acceda debe tener un programa especial que reciba y gestione las conexiones. El puerto que se utiliza generalmente es el 23.

Traffic Shapping.- Es un intento para controlar el tráfico de una red de computadores para optimizar o garantizar su funcionamiento, las bajas latencias, etc... Así, proporciona un mecanismo para controlar el volumen de tráfico que es enviado en una red así como su frecuencia. Aunque es un método para mejorar los protocolos de red, puede ser utilizado para limitar cierto tipo de paquetes o tráfico desde un punto a otro.

TTL.- Tiempo de Vida o Time To Live, es un concepto usado en redes de computadores para indicar por cuántos nodos puede pasar un paquete antes de

ser descartado por la red o devuelto a su origen. El TTL como tal es un campo en la estructura del paquete del protocolo IP. Sin este campo, paquetes enviados a través rutas no existentes, o a direcciones erróneas, estarían vagando por la red de manera infinita, utilizando ancho de banda sin una razón positiva.

UDP.- User Datagram Protocol, es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación, ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco se sabe si ha llegado correctamente, ya que no hay confirmación de entrega o de recepción.

Virus.- es un programa que permanece oculto, reproduciéndose hasta que se activa y causa daño.

Virus Macro.- Se llaman macros las secuencias de instrucciones que el usuario de un programa puede escribir y almacenar para realizar tareas complejas o repetitivas. Los virus de macro utilizan la potencia y las funciones integradas en la aplicación para duplicarse y propagarse. A diferencia de los virus ordinarios, los virus de macro no infectan programas, infectan documentos.

Wildcard.- sirve para bloquear el contenido de páginas web que empiecen con la expresión ingresada en este campo.

BIBLIOGRAFIA

Libros o Manuales

Tema: IPS

- Autor: Fortinet
  Título: FortiGate IPS Guide
  Fecha de Edición: Noviembre 2004

Tema: Firewall

- Autor: Fortinet
  Título: FortiGate-60 Install & Config Guide
  Fecha de Edición: Agosto 2003

Tema: FortiGuard Center

- Autor: Fortinet
  Título: FortiGuard Web Content Filtering
  Fecha de Edición: Agosto 2003

Páginas Web

Tema: Virus Informáticos

- Autor: Monografías.com
  Página Web: http://www.monografias.com/trabajos15/virus-informatico/virus-informatico.shtml
  Fecha de Consulta: Febrero/2006
- Autor: PandaSoftware
  Página Web:
  http://www.pandasoftware.es/virus_info/about_virus/information3.htm
  Fecha de Consulta: Febrero/2006
- Autor: Alerta Antivirs
  Página Web:
  http://alerta-antivirus.red.es/virus/ver_pag.html?tema=V&articulo=1&pagina=2
  Fecha de Consulta: Abril/2006

Tema: Vulnerabilidades de los protocolos de comunicación

- Autor: Vsantivirus
  Página Web: http://www.vsantivirus.com/ev-vul-tcp.htm

Fecha de Consulta: Marzo/2006

Tema: Spam

- Autor: Symatec
  Página Web:
  http://www.symantec.com/region/mx/smallbusiness/articles/LAM_ispam.html
  Fecha de Consulta: Abril/2006

Tema: Seguridad en Redes

- Autor: Symatec
  Página Web:
  http://www.symantec.com/region/mx/smallbusiness/articles/LAM_insider.html
  Fecha de Consulta: Febrero/2006
- Autor: Symatec
  Página Web:
  http://www.symantec.com/region/mx/smallbusiness/articles/LAM_depth.html
  Fecha de Consulta: Febrero/2006
- Autor: ArCERT Coordinación de Emergencias en Redes Teleinformáticas
  Página Web:
  http://www.arcert.gov.ar/webs/manual/manual_de_seguridad.pdf
  Fecha de Consulta: Abril/2006

Tema: Tipos de Ataques

- Autor: Ingeniería Dric soluciones Integrales TI
  Página Web: http://www.dric.com.mx/seguridad/di/di4.php?cat=7
  Fecha de Consulta: Febrero/2006
- Autor: Kernelnet Informática
  Página Web: http://www.kernelnet.com/content/view/172/2/
  Fecha de Consulta: Abril/2006

Tema: IDS

- Autor: Maestros del Web
  Página Web: http://www.maestrosdelweb.com/editorial/snort/
  Fecha de Consulta: Marzo/2006

Tema: IPS

- Autor: b:Secure
  Página Web:

http://www.bsecure.com.mx/articulos.php?id_sec=48&id_art=4817&num_page=21055

Fecha de Consulta: Enero/2007

Tema: Antivirus

- Autor: Per Antivirus

  Página Web: http://www.perantivirus.com/antivir.htm

  Fecha de Consulta: Febrero/2006

- Autor: PandaSoftware

  Página Web: http://www.pandasoftware.es/productos/activescan

  Fecha de Consulta: Mayo/2006

Tema: Firewall

- Autor: Microsoft

  Página Web:

  http://www.microsoft.com/latam/seguridad/hogar/articulos/firewall.asp

  Fecha de Consulta: Febrero/2006

- Autor: Monografías.com

  Página Web:

  http://www.monografias.com/trabajos3/firewalls/firewalls.shtml

  Fecha de Consulta: Febrero/2006

- Autor: Revista RedEscolar

  Página Web:

  http://redescolar.ilce.edu.mx/redescolar/Revista/10/articulos/08.html

  Fecha de Consulta: Mayo/2006