UNIVERSIDAD DE LAS AMÉRICAS

INGENIERÍA DE SISTEMAS EN COMPUTACIÓN EN INFORMÁTICA

TECNOLOGÍA VPN-1/FIREWALL-1 NG DE CHECK POINT IMPLEMENTADA PARA ESTABLECER SEGURIDAD EN COMUNICACIONES REMOTAS EN UNA COMPANÍA ENCARGADA DE GERENCIAR Y ADMINISTRAR LOS HOTELES MARRIOTT.

TRABAJO DE TITULACIÓN PRESENTADO EN CONFORMIDAD A LOS REQUISITOS PARA OBTENER EL TITULO DE INGENIERO DE SISTEMAS EN COMPUTACIÓN E INFORMÁTICA

DIRECTOR: ING. XAVIER ARMENDÁRIZ MBA

AUTOR: JUAN JOSÉ GARCÍA

QUITO - 2007

DECLARACIÓN PROFESOR GUIA

Declaro que el trabajo de titulación “Tecnología VPN-1/Firewall-1 NG de Check Point implementada para establecer seguridad en comunicaciones remotas en una compañía encargada de gerenciar y administrar los hoteles Marriott” fue realizado por el alumno Juan José García Vélez, alumno de la Facultad de Ingeniería, en la Carrera de Sistemas de Computación e Informática; quien estuvo bajo mi orientación y guía.

Es todo cuanto puedo decir en honor a la verdad.

Ing. Xavier Armendáriz, MBA

Profesor Guía

AGRADECIMIENTOS

Agradezco a la Universidad de lasa Américas y a los profesores que a lo largo de estos años me supieron guiar para poder alcanzar un desarrollo profesional y humano que ha sido clave en mi vida profesional. Al Ing. Xavier Armendáriz MBA, que a pesar de la distancia y las dificultades que el estar lejos representa, me ha apoyado y me ha dado una mano incondicional no solo como profesor, tutor, guía, sino como amigo.

A mis padres que me han apoyado en cada paso de mi vida, a la ayuda que he recibido de mis hermanos y a mis compañeros de carrera que son parte importante de este logro tan importante.

Al Grupo MDM que me facilitó los estudios y prácticas para realizar este proyecto de titilación.

A mi esposa e hijos que han sido mi inspiración para poder culminar mis años de estudio y han estado ahí para no dejarme desmayar.

Por ultimo a Dios que sin El nada habría sido posible ya que el puso a todas estas personas en mi vida, llenándola de felicidad y bendiciones.

A mis hijos Juan José, Sophía Isabella y a mi esposa Claudia

Porque son mis ángeles, mi alegría,

mi razón de vivir e inspiración para poder

ser cada vez una mejor persona.

RESUMEN

El Grupo MDM es el encargado de administrar y gerenciar una franquicia compuesta por tres hoteles de la corporación Marriott, y tiene la necesidad de protegerse de ataques con una herramienta donde el costo beneficio sea un punto importante pero donde el punto más susceptible y decisivo es resguardar de manera confiable la seguridad de su información.

Es importante que los usuarios remotos sean capaces de conectarse a la red interna de la organización desde cualquier parte del mundo sin ningún inconveniente. Estos usuarios necesitan una herramienta que sea amigable y no arroje complicaciones, sino que sea prácticamente invisible para lo mismos, otorgándoles la tranquilidad de saber que su información está a salvo de ataques e intercepciones que pongan en riesgo su información.

Con estos requisitos, Firewall-1/VPN-1, de Check Point, fue seleccionado entre varios productos que ofrecen protección sobre equipos y aplicaciones que trabajan expuestos al Internet, para ser implementado por los administradores de red del Grupo MDM. El estudio de autenticación y cifrado son claves al momento de seleccionar esta herramienta ya que no se debe descuidar el más mínimo detalle que pueda exponer la seguridad de la información.

Como resultado de la implementación se tiene un sistema seguro y confiable que brinda facilidad de administrar las diferentes redes, equipos y usuarios, donde se puede aislar un equipo afectado ocasionado por un tipo de ataque malicioso.

Índice

I. Introducción 8

II. Marco Teórico

a. Seguridad en el Internet. 11

b. VPN y FireWall. 14

c. Estudio del manejo de un sistema de seguridad Check Point. 20

III. Análisis de VPN-1/FireWall-1 en plataformas Windows NT/2000 33

IV. Políticas de seguridad y estándares implementados por Check Point aplicados en la tecnología VPN-1/FireWall-1

a. Análisis de la autenticación en un VPN-1. 42

b. Análisis de la encriptación en un VPN-1. 52

c. Análisis de las políticas de seguridad utilizadas por VPN-1 /FireWall-1 de CheckPoint. 64

d. Estudio de los estándares de seguridad en un VPN-1/FireWall-1 de CheckPoint. 70

V. Prototipo de la red virtual (VPN-1) /FireWall-1 de CheckPoint en el Grupo MDM

a. Diseño de VPN-1/FireWall-1 de Check Point implementado por el Grupo MDM. 78

b. Arquitectura de VPN-1/FireWall-1 de Check

Point implementado por el Grupo MDM. 80

c. Políticas de seguridad utilizadas por el Grupo MDM. 82

d. Implementación del prototipo. 94

VI. Conclusiones 127

VII. Bibliografía 131

VIII. Anexos 133

1. Introducción

La tecnología de Internet ha provocado que muchas empresas tengan que volver a definir la forma en que se comunican con sus clientes, cómo trabajan con sus socios y cómo venden sus productos. A medida que una empresa vaya introduciéndose en Internet para elaborar nuevos modelos de actividad comercial, la seguridad en ese entorno y la fiabilidad de la red se irán haciendo cada vez más importante por lo que se debe garantizar que los datos, las aplicaciones, los servidores y las redes estén protegidos frente a los ataques que acechan desde Internet.

La constante intromisión de personas ajenas a la información, ha motivado a las companías adoptar todas las medidas de seguridad pertinentes. Las redes deben cumplir con atributos tales como seguridad, fiabilidad, alcance geográfico y efectividad en costos para poder proteger la información. Se ha demostrado que las redes reducen tiempo y dinero en los gastos de las empresas, lo que significa una gran ventaja para las organizaciones que cuentan con oficinas remotas. Para que funcione la seguridad informática en una empresa es imprescindible que se describan políticas y procedimientos en materia de seguridad que se conozcan y se hagan cumplir en todo nivel.

La conectividad inmediata de las computadoras y servidores se convierte en un problema para los administradores de red y seguridad informática.

Las empresas con intranets poseen una gran cantidad de información confidencial en línea; el mal manejo de esta información puede ocasionar graves daños y pérdidas a las companías. Otro peligro es la infiltración de virus, spams y gusanos entre otros, los cuales pueden abrir orificios y violar la seguridad, destruir los datos de las companías y hacer que los administradores pierdan tiempo tratando de arreglar el daño ocasionado. Generalmente estos ataques se producen por los mismos empleados que bajan y trabajan con programas sin control, desconociendo las reglas de la empresa, con una mentalidad inocente de que no sucederá nada.

Los Firewall son una forma de protección que obliga a que todo el tráfico de una o varias redes locales conectadas pasen a través de un puente de control. El Firewall puede ser un software, hardware o una combinación de ambos. Utilizando la inspección de estado, FireWall-1 de Check Point integra la protección de nivel de red y la de nivel de aplicación. Como solución de seguridad en Internet, FireWall-1 proporciona un gran nivel de seguridad, con control de acceso, protección contra ataques, seguridad de contenidos, autentificación y conversión de dirección de red (NAT) integrada. FireWall-1 se basa en la administración inteligente, y permite administrar de la misma forma la infraestructura de seguridad con la máxima eficiencia.

A continuación se presenta un documento donde se analiza, estudia y se muestra un prototipo de una tecnología de seguridades para

comunicaciones remotas FireWall-1/VPN-1 implementado en el Grupo MDM encargado de administrar los hoteles Miami Dadeland Marriott, Courtyard Dadeland by Marriott y JW Marriott Miami.

Con esta implementación se intenta lograr una independencia de la corporación Marriott. Esta ha venido administrando todos los servidores de las tres propiedades. No se puede, ni es el intento lograr una independencia absoluta ya que la corporación Marriott posee sus propios servidores en cada una de las propiedades que tienen su nombre, más sin embargo se intenta tener control de los servidores y las redes administrativas del Grupo MDM, que estarán administrados y bajo la protección de la aplicación Firewall-1/VPN-1.

2. Marco Teórico

2.1 Seguridad en el Internet

Para comenzar el análisis de seguridad en el Internet se debe conocer las características de lo que se pretende proteger. En este caso la información. El concepto dice que información "es un conjunto ordenado de datos los cuales son manejados según la necesidad del usuario. Para que un conjunto de datos pueda ser procesado eficientemente y pueda dar lugar a información, primero se debe guardar lógicamente en archivos"[1].

Establecer el valor real de la información es algo relativo ya que en muchos casos no se la valora adecuadamente debido a su intangibilidad. En el caso de la información privada se debe hacer especial énfasis en preservarla como tal conservando las siguientes características: Integridad, Operatividad, Confidencialidad, Control y Autenticidad.

Dentro del entorno informático, amenaza "es cualquier elemento que comprometa al sistema"[2]. Las amenazas pueden ser analizadas en tres instancias: antes, durante y después del ataque. Dentro de cada etapa se deben realizar las siguientes acciones:

[1] http://comunisfera.blogspot.com/2006/09/definiciones-de-informacin-y-documento.html
[2] www.segu-info.com.ar/tesis/cap1.pdf pag. 7

- Prevención (antes)
- Detección (durante)
- Recuperación (después)

La seguridad indica el porcentaje en que un sistema informático se encuentra libre de daño y riesgo. Es muy difícil conseguir que este porcentaje llegue a un 100% y es por esto que se habla de fiabilidad de un sistema más que seguridad del mismo. Se define fiabilidad como "la habilidad de un sistema de realizar una función requerida en determinadas condiciones y durante un cierto periodo de tiempo"[3].

Para llevar a cabo un ataque se necesita de tres elementos: motivación, capacidad y oportunidad. Si el ataque es sobre los límites físicos de una organización, se necesita además tener un tipo especial de personalidad. Es por todos conocidos la existencia de grupos organizados dedicados a sustraer y boicotear información y servicios que dependen de controles tecnológicos. Estos grupos son conocidos como:

- Hacker
- Cracker
- Pirata Informático

[3] HUERTA, Antonio Villalón. "Seguridad en Unix y Redes". Versión 1.2 Digital – Open Publication License v.10.2 de Octubre de 2000. *www.kriptopolis.com*

- Lammers
- Samurai

Es necesario recordar que existen todavía grandes vacíos legales acerca del delito informático, por lo que la motivación de vulnerar sistemas informáticos tiene desde el punto de vista legal y moral, menos razones para inhibirse. Un ataque es “un intento de acceso o uso desautorizado de un recurso”[4]. Un incidente envuelve un conjunto de ataques que pueden ser distinguidos de otro grupo por sus características tales como: grado, similitud, técnicas utilizadas, tiempos de ataque, etc. La identificación de una amenaza requiere conocer los tipos de ataques, el tipo de acceso, la forma operacional y los objetivos del atacante. Las consecuencias de los ataques se pueden agrupar en:

- Corrupción de Información: La información que no contenía defectos, pasa a tenerlos.
- Negación de Servicio (DoS): servicios que deberían estar disponibles no lo están.
- Destino errado: los datos llegan a destinos a los que no deberían llegar.

Los métodos de ataque más conocidos son los siguientes:

[4] www.segu-info.com.ar/tesis/cap7.pdf

- Ingeniería Social
- Escuchar trafico de paquetes ajenos
- Caballos de Troya
- Bombas Lógicas
- Difusión de Virus
- Obtención de Contraseñas, Códigos y Claves

2.2 VPN y FireWall

2.2.1 Firewall

Un Cortafuegos o Firewall es un sistema ubicado entre dos redes cuyo trabajo es el de hacer cumplir una política de seguridad. Es el mecanismo encargado de proteger una red confiable de una no confiable.

El Firewall determina cuáles de los servicios de la red pueden ser accesados. Para que un Firewall sea efectivo, todo tráfico de información del Internet debe pasar a través del mismo donde la información podrá ser inspeccionada. El Firewall únicamente puede autorizar el paso del tráfico. Desafortunadamente, este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece en torno a él.

2.2.1.1 Tipos de Firewall

Entre los varios tipos de Firewall se encuentran los siguientes:

- Filtrado de Paquetes: Se utilizan ruteadores con filtros y reglas basadas en políticas de control de acceso.
- Proxy-Gateways de Aplicaciones: Para evitar las debilidades asociadas al filtrado de paquetes, se desarrolló un software de aplicación encargado de filtrar las conexiones. Estas aplicaciones son conocidas como Servidores Proxy y la máquina donde se ejecuta recibe el nombre de Gateway de Aplicación o Bastión Host.
- Dual-Homed Host: Son dispositivos que están conectados al perímetro interior y exterior y no dejan pasar paquetes IP como sucede en el caso del Filtrado de Paquetes.

- Screened Host: Se combina un ruteador con un bastión host y el principal nivel de seguridad proviene del filtrado de paquetes.
- Screened Subset: Con este diseño se intenta aislar del Firewall al Nodo Bastión, que es la máquina más atacada y vulnerable. Para esto se establece una Zona Desmilitarizada (DMZ) de forma tal que sin un intruso accede a esta máquina no consiga el acceso total a la subred protegida.
- Inspección de Paquetes: Este tipo de Firewall se basa en el principio de que cada paquete que circula por la red es inspeccionado, al igual que su procedencia y destino. Se aplican desde la capa de Red hasta la de Aplicaciones. Generalmente son instalados cuando se requiere seguridad sensible al contexto y en aplicaciones muy complejas.

- Firewalls Personales: Estos Firewalls son aplicaciones para usuarios finales que desean conectarse a una red externa insegura y mantener su computadora a salvo de ataques.

2.2.2 VPN – Redes Privadas Virtuales

En cuanto a la tecnología de Redes Privadas Virtuales (VPN), estas proporcionan un medio seguro para usar un canal público del Internet como el medio necesario para transmitir datos privados. Con tecnologías de encriptación y encapsulamiento, una VPN crea un túnel privado a través de un medio inseguro.

Las VPN también permiten la conexión de usuarios móviles a una red privada, tal como si estuvieran en una LAN. Esto resulta muy conveniente para personal que no tiene lugar fijo de trabajo dentro de la empresa, como podrían administradores de red que controlan su trabajo cuando no se encuentran físicamente presentes.

En el modo de tecnología de túneles los datos se transfieren siendo insertados dentro de un paquete de datos de un protocolo específico. Al llegar al destino, el paquete es

desempaquetado volviendo así a su estado original. En el traslado a través de Internet, los paquetes viajan encriptados.

Las técnicas de autenticación son esenciales en las VPN, ya que aseguran a los usuarios que están intercambiando información con el destino o dispositivo correcto. La autenticación en VPN es parecida al proceso de acceso a un sistema con un nombre de usuario y contraseña, pero con necesidades mayores de validación de identidades. La mayoría de los sistemas de autenticación usados en VPN están basados en un sistema de claves compartidas.

La autenticación es llevada a cabo generalmente al inicio de una sesión, y luego aleatoriamente durante su funcionamiento, para asegurar que no haya algún tercer participante que se haya entrometido en la conversación. La autenticación también es utilizada para asegurar la integridad de los datos.

Todas las Redes Privadas Virtuales tienen algún tipo de tecnología de encriptación que esencialmente empaqueta los datos en un paquete seguro. La encriptación es considerada tan esencial como la autenticación, ya que protege los datos transportados de poder ser vistos y entendidos en el viaje de un extremo a otro de la conexión. Existen dos tipos de

técnicas de encriptación que se usan en las VPN: encriptación de clave secreta, o privada, y encriptación de clave pública.

En las VPN, la encriptación debe ser realizada en tiempo real. El protocolo más usado para la encriptación dentro de las VPN es IPSec, que consiste en un protocolo de red seguro para IPv4 e IPv6. IPSec provee encriptación a nivel de red.

El método de túneles es una manera de crear una red privada. Permite encapsular paquetes dentro de paquetes para acomodar protocolos incompatibles[5]. Dentro de los protocolos que se usan para la metodología de túneles se encuentra el Protocolo de Túnel de Punto a Punto (PPTP), y el modo túnel de IPSec entre otros.

Los requerimientos para que una Red Privada Virtual cumpla con sus objetivos de seguridad de transmisión son:

- Escalabilidad
- Performance
- Disponibilidad
- Transparencia
- Fácil de Administrar
- Interoperatividad

[5] RATCLIFFE, Andrew*;* SHAH Inti; *Check Point VPN-1/FireWall-1 NG Administration;* Editorial McGraw Hill; 2002. pag.: 350

- Encriptación
- Seguridad

2.3 Estudio del manejo de un sistema de seguridad Check Point

El FireWall-1 desarrollado por la empresa israelí Check Point Software Technologies Ltd. es quizás el más utilizado en los Estados Unidos y Europa. Este firewall se ejecuta sobre diferentes sistemas Unix, así como sobre Windows

Quizás la característica más importante de Firewall-1 es que incorpora una nueva arquitectura dentro del mundo de los cortafuegos: la inspección con estado[6]. Firewall-1 inserta un módulo denominado Módulo de Inspección en el núcleo del Sistema Operativo sobre el que se instala, en el nivel software más bajo posible por debajo inclusive del nivel de red. Desde ese nivel el sistema de Check Point puede interceptar y analizar todos los paquetes antes de que lleguen al resto del sistema con lo que se garantiza que ningún paquete es procesado por ninguno de los protocolos superiores hasta que FireWall-1 compruebe que no viola las políticas de seguridad definidas en el Firewall. La tecnología de

[6] http://www.checkpoint.com/support/technical/documents/docs_vpn_fw.html

Check Point, Firewall-1 es capaz de analizar la información de un paquete en cada uno de los siete niveles OSI y a la vez es capaz de analizar la información de estado registrada de anteriores comunicaciones. FireWall-1 entiende la estructura de los diferentes protocolos TCP/IP, incluso de los ubicados en la capa de aplicación, de manera que el Módulo de Inspección extrae la información relevante de cada paquete para construir tablas dinámicas que se actualizan constantemente, tablas que el firewall utiliza para analizar comunicaciones posteriores.

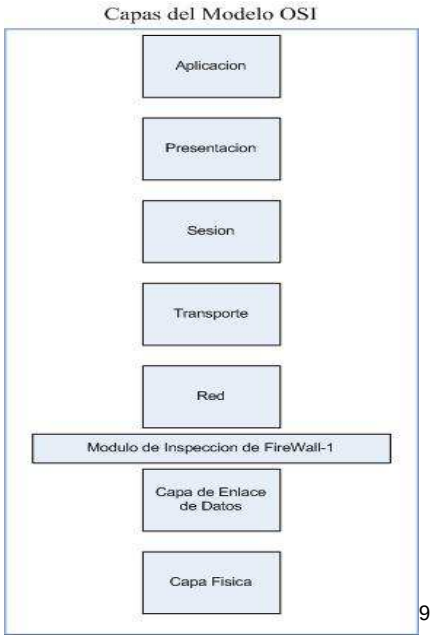
En el Módulo de Inspección se implantan las políticas de seguridad definidas en cada organización mediante un sencillo lenguaje denominado Inspección, también diseñado por Check Point Software Technologies. Desde una interfaz muy amigable se genera un código en este lenguaje, que se compila y se inserta en el Módulo de Inspección.

En cuanto a la arquitectura de Firewall-1 se refiere, el sistema de Check Point está basado en dos módulos independientes: de gestión o control y de cortafuegos[7]. El primero de ellos está formado por el gestor gráfico de políticas incluyendo el visor de registros y el segundo es el servidor de gestión. El gestor gráfico puede ser un cliente Unix o un servidor Windows. Debido a que no existe un

[7] http://es.tldp.org/Manuales-LuCAS/SEGUNIX/unixsec-2.1-html/node244.html

cliente gráfico para Linux, se tiende que la mayoría de clientes de Check Point tiendan a utilizar plataformas Windows para gestionar un firewall, tal como se lo hace el Grupo MDM. El gestor gráfico puede ejecutarse en la misma máquina que el servidor de gestión o en una diferente, mediante un esquema cliente/servidor. Este gestor no hace más que presentar de una forma cómoda al administrador del firewall la información generada por el servidor de gestión, que es el verdadero núcleo de gestión del firewall el cual permite administrar diferentes sistemas con módulo de firewall desde una misma estación de control. La aplicación Firewall-1/VPN-1 ofrece una mayor capacidad de procesamiento con un tamaño compacto y fácil de instalar que soporta hasta 600.000 sesiones y 50.000 túneles VPN al mismo tiempo[8]. Dichas aplicaciones se caracterizan por tiempos de latencia muy bajos, lo que las hace idóneas para seguridad en comunicaciones multimedia, y su rendimiento no se ve afectado por las normas de seguridad firewall.

[8] http://www.portalx.com.uy/cgi/portalx/Hecon01.EXE?O,0,,0,10310,10301,1039301,2



[9]

Gráfico 1

Por otra parte, el módulo de cortafuegos está formado por el módulo de inspección, los diferentes servicios de Firewall-1 y los servidores de seguridad del firewall. El módulo de inspección se instala como se muestra en el Gráfico 1, entre el nivel de enlace y el nivel de red, por completo antes de la pila de protocolos TCP/IP, con lo que se asegura que Firewall-1 analiza todos y cada uno de los paquetes que pasan por el sistema. Los servicios del firewall son simples programas con diferentes funciones, como la comunicación con el servidor de gestión o la carga de las reglas definidas para el firewall en el módulo de inspección. Finalmente, los servidores de seguridad son módulos que se invocan cuando así se define en la política, y que realizan tareas de autenticación y seguridad de contenidos; la

[9] http://www.checkpoint.com/support/technical/online_ug/firewall-14.0/glossary.htm

conexión entre origen y destino se divide en dos, una entre el origen y el servidor de seguridad y otra entre este y el destino.

Como cualquier otro sistema cortafuegos, Firewall-1 permite al administrador de la red definir una política de seguridad formada por reglas, cada una de las cuales se basa principalmente en el origen, destino y servicio de una determinada trama.

La gestión de Firewall-1 en Windows es completamente gráfica, a través de dos interfaces principales:

1. De gestión de políticas
2. El visor de registros

Sin embargo, siempre existe la opción de trabajar en modo texto aunque esta opción no suele ser la habitual entre los administradores de Firewall.

2.3.1 Administración del Firewall

Para administrar el firewall, cada uno de los administradores definidos puede conectar desde las máquinas autorizadas al servidor de gestión que es la máquina en la que se instala el módulo de administración de Firewall-1, para lo cual necesita autenticarse mediante su nombre de usuario y su clave. Una

vez conectado, puede comenzar a trabajar con FireWall-1. Desde el editor gráfico, las políticas se ven como un conjunto de reglas que se examina de arriba a abajo hasta que una de ellas se empareje con el paquete que se está analizando. Cada una de estas reglas está numerada en función del orden de aplicación, y sus campos principales son los habituales en cualquier firewall:

- Origen
- Destino
- Servicio
- Acción

Gráfico 2

Además, existen un campo que indica si se ha de rastrear la acción, otro para determinar dónde se ha de instalar, otro para especificar el tiempo y la fecha en que la regla estará activa y finalmente un campo de texto donde se pueden incluir comentarios.

Como sucede en todo firewall, tanto el campo origen como el destino pueden ser sistemas concretos o redes completas. En Firewall-1 ambos elementos, así como los servicios, se manejan como objetos los cuales son elementos definidos por el administrador e identificados mediante un nombre fácilmente identificable por el mismo, con una serie de propiedades determinadas. En el caso de los máquinas o las redes la propiedad más importante es la dirección de red con su máscara correspondiente asociadas al objeto; en el caso de los servicios, definidos también por un nombre, la característica más importante es el puerto o rango de puertos asociado al mismo. Por ejemplo, se puede definir el objeto servidor1, con su dirección de red correspondiente, el objeto DMZ, con su dirección de red y máscara asociada, o el objeto SSH, con su puerto concreto. En todos los casos, el nombre dice mucho más al encargado de administrar el firewall que una simple dirección de red o número de puerto, lo que facilita enormemente la administración del firewall.

El campo Acción de cada regla define qué se hace con una conexión cuando se empareja con la regla. En Firewall-1, sin tres las acciones principales que se toman:

- Aceptar: Establecer la conexión a través del firewall.
- Rechazar: Rechazar la conexión notificando al origen,
- Negar: Rechazar la conexión sin notificarlo al origen.

Gráfico 3

En cuanto a los diferentes productos existentes en el mercado los principales competidores del Firewall-1/VPN-1 de Check Point son Juniper NetScreen y Cisco PIX.

Analizando los costos entre ellos, ofreciendo productos con servicios y número de usuarios similares, se presenta en la siguiente tabla la gran ventaja que tiene Check Point sobre su competencia[10]:

	Check Point Firewall-1/VPN-1	**Júpiter NetScreen 204/Juniper IDP-10**	**Cisco Pix 515E/Cisco IDS 4215**
Gateway			
Firewall / VPN	SW: $6,500	$11,500	$7,495

[10] The Tolly Group, The Authoritative, unbiased source for IT certification, research and testing. Improving Security ROI via Integrated Application Security Solution. White Paper. Febrero 2005. pag.: 12

	HW: $1,595		
IPS (Sistema de Prevension anti Intrusos)	Incluido	$9,195	$8,000
Suscripción a Servicios			
Firewall / VPN	Servicio SmartDefense $1,000	$920	No disponible
IPS	Incluido	Incluidos algunos servicios en los costos de IDP-10	Incluidos en los costos de IDS 4215
Soporte			
Firewall / VPN	Incluido	$1,040	$ 900
IPS	$975	Incluido	$ 700
Total	***$10,070***	***$ 22, 655***	***$ 17, 095***

Cabe resaltar que el Firewall-1/VPN-1 de Check Point tiene una participación igual al 65% del mercado en lo que se refiere a Firewall dedicado a proteger edificios con muchos usuarios. Como se muestra en el Gráfico 4, con más de 100 millones de usuarios en todo el mundo, mientras que sus principales competidores más otros productos existentes en el mercado tales como Sonicwall, Lucent Technologies, Novel Networks, Watchguard Technologies, se reparten el 35%

restante lo que hace de Check Point un software fiable en este tipo de aplicaciones.

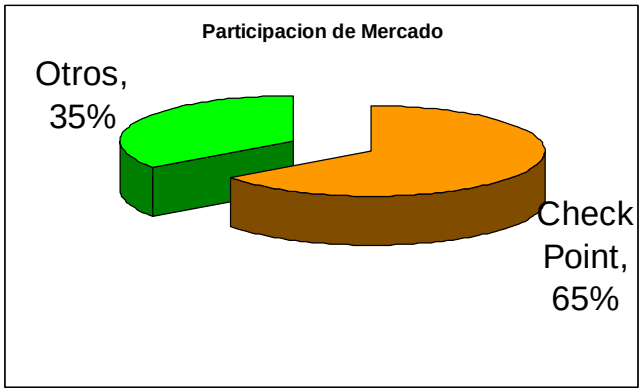


Gráfico 4

Sin embargo, otras pruebas realizadas muestran que existen otras marcas en el mercado que se hacen fuertes donde Check Point no lo es. Con una evaluación de 16 cortafuegos realizada por Opus One, miembro de la Network World Global Test Alliance, junto con Spirent Communications interaron determinar de forma precisa la rapidez de los productos hoy en el mercado. Los productos analizados fueron: PIX 525 de Cisco, Firewall-1 de Check Point, eTrust de Computer Associates, eTrust de Computer Associates, KnightStar de CyberGuard, Enternet Firewall de Enternet, Brick de Lucent, NetScreen-100 de NetScreen, Network-1 de CyberwallPlus, WebShield de Network Associates, BorderManager de Novell, IP650 de Nokia , SideWinder de Secure Computing, SonicWall Pro VX de SonicWall, Raptor de Symantec, AppSwitch 3500

de TopLayer y Firebox II de WatchGuard. Los productos de NetScreen, Cisco y CyberGuard reportaron el mayor rendimiento.

Concretamente, los equipos de NetScreen, Cisco y CyberGuard alcanzaron las más altas capacidades de proceso. NetScreen ofreció un rendimiento total excepcional con cifras consistentemente elevadas en todas las pruebas.

En las pruebas basadas en la conexión, cada producto debía ser capaz de manejar múltiples reglas de cortafuegos con al menos 100 reglas en cada producto. Para algunos, como los de TopLayer y Check Point, la imposición de estas normas no fue un gran impacto porque estos dispositivos crean reglas dinámicas para conexiones que aceleran el procesamiento una vez ha sido establecida la conexión TCP. Por el contrario, en el caso de los cortafuegos basados en el filtrado de paquetes que son incapaces de modificar dinámicamente las reglas, como Novell y CyberGuard, la adición de reglas tuvo un mayor impacto sobre el rendimiento.

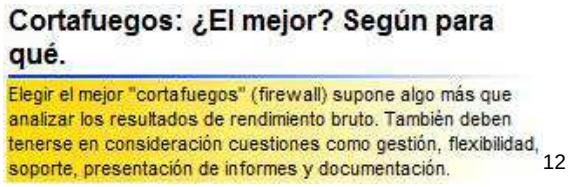
En lo que a número de usuarios se refiere, un cortafuegos al que no afectara si estaba inspeccionando una o mil conexiones, debería proporcionar un rendimiento

aproximadamente similar para cargas baja, moderada y alta. A altas velocidades, Nokia, NetScreen, CheckPoint y Cisco fueron los que demostraron el mejor rendimiento total. Si se desea proteger un edificio alimentado por un circuito de 45 Mbps con aproximadamente 1000 usuarios, y que el cortafuegos llegue un flujo mayor, la opción más indicada serán los productos de Cisco, CyberGuard, Check Point, NetScreen, Network Associates, Nokia y Ethernet.

Los resultados en rendimiento bruto, es decir, si estuviera gestionando una gran cantidad de hospedaje Web, sólo tres fabricantes lograron una presencia consistente en las principales cinco clasificaciones de rendimiento: Cisco, CyberGuard y NetScreen. Cisco recibió la mejor puntuación en la tabla de rendimiento agregado en todas las pruebas y es siempre una apuesta segura.

Aunque el mejor producto en rendimiento en cada prueba era una plataforma de hardware dedicada, los cortafuegos que corren sobre sistemas operativos de propósito general lograron ocupar puestos altos en la clasificación. Por ejemplo, KnightStar, de CyberGuard, y SideWinder, pasaron paquetes en bruto más rápido que FireBox, de WatchGuard y SonicWall.

Productos como Firewall-1 de Check Point y WebShield de Network Associates, aunque destacaron entre los mejores en las pruebas de protección, no fue del todo positivo cuando se analizó su adecuación para otras tareas, como la transmisión de paquetes en bruto. Este hecho pone de relieve que es fundamental la comprensión por el administrador de las peculiaridades de su red antes de tomar una decisión de compra[11].


Cortafuegos: ¿El mejor? Según para qué.

Elegir el mejor "cortafuegos" (firewall) supone algo más que analizar los resultados de rendimiento bruto. También deben tenerse en consideración cuestiones como gestión, flexibilidad, soporte, presentación de informes y documentación. [12]

Gráfico 5

[11] http://www.portalx.com.uy/cgi/portalx/Hecon01.EXE?O,0,,0,10310,10301,1039301,2
[12] Ibid

3. Análisis de VPN-1/FireWall-1 en plataformas Windows NT/2000

Una vez analizado que Check Point es una de las plataformas indicadas para ser implementada en los edificios del Grupo MDM, el primer paso antes de la instalación del firewall es la selección del Sistema Operativo en el cual va se va a desenvolver. En este caso se ha seleccionado las plataformas Windows NT/2000 ya que es política del Grupo MDM utilizar únicamente plataformas Windows.

Es preciso indicar que ningún Sistema Operativo es mejor o peor para determinados ambientes. El punto de partida para escoger el Sistema Operativo se basa en la capacidad y conocimiento de sus administradores, así como las políticas internas de la empresa. La seguridad y estabilidad del firewall va a depender de una configuración correcta del Sistema Operativo.

El Firewall-1 de Check Point puede ser instalado en Windows NT o Windows 2000 Server/Advanced Server o en la nueva familia para servidores Windows 2003.

Las ventajas de utilizar el Firewall-1-VPN-1 de Check Point con Windows son las siguientes:

- Es fácil de utilizar
- Fue uno de los primeros en ser utilizado por Check Point
- Existe mucho software complementario proveniente de terceros

Desventajas:

- En Windows NT resulta más complicada su administración remota ya que se precisa de una buena interfaz grafica. Esto mejora para Windows 2000 Server y desaparece en la nueva familia de servidores Windows 2003.

La instalación del Sistema Operativo tiene que ser hecha por el administrador y no utilizar discos ya instalados con versiones anteriores. Solo empezando completamente desde cero se conoce realmente cómo está instalado el Sistema Operativo y qué servicios se los agregó y cuáles no. No es recomendable tener una conexión al Internet durante la instalación del sistema ya que esto puede traer y causar muchos riesgos. Si se necesita instalar actualizaciones o parches, es mejor descargarlos por intermedio de otra máquina, crear un CD instalador e instalarlos por este medio.

Una vez instalado el Sistema Operativo, el siguiente paso es ambientarlo a la red local. Esto consiste en agregar cuentas del sistema y todas las configuraciones de red incluyendo direcciones DNS. Es el Sistema Operativo el encargado de toda la red y el ruteo y no el Firewall. El Firewall determina únicamente qué puede y qué no puede suceder. Una vez que la sesión sea autentificada y aprobada por el Firewall, depende del Sistema Operativo enviar los paquetes al destinatario correcto.

El acceso al Sistema Operativo debe ser limitado en cuanto al número de usuarios. La gente que tiene acceso al sistema debe ser de absoluta

confianza, responsabilidad y conocimiento tal capaz de informar y actuar a tiempo en caso de algún ataque o caída imprevista del Sistema Operativo. Las cuentas deben tener contraseñas seguras difícil de descifrarlas y las cuentas deben ser locales del sistema más no cuentas del dominio tales como las cuentas de acceso a domino de Windows NT.

Una vez que se cuenta con una correcta instalación, configuración y seguridad del Sistema Operativo, se continúa con la instalación del Firewall-1. El proceso de instalación es muy sencillo y se despliega un cuadro de diálogo que sirve de guía durante todo el proceso.

Cuando se llega a la pantalla que muestra el Gráfico 6 , donde se indican los “clientes” que representan los iconos que se van a tener dentro del programa de Check Point en Windows representando las diferentes opciones que el programa presenta. Por defecto se encuentran todos seleccionados pero en el caso de no querer contar con alguno de ellos se los debe quitar la selección.

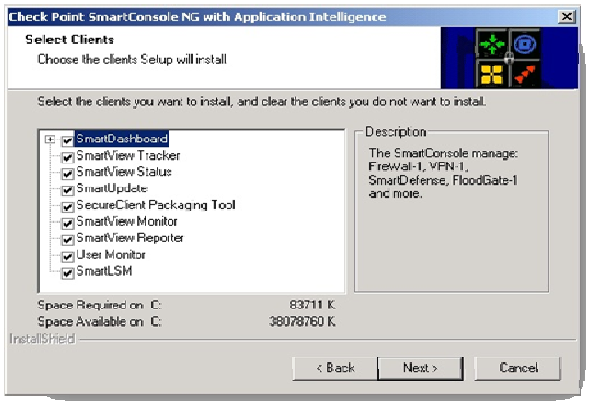


Gráfico 6

Durante el proceso de instalación se ingresan la o las licencias obtenidas para contar con una completa instalación del programa de Check Point, tal como muestra el Gráfico 7.

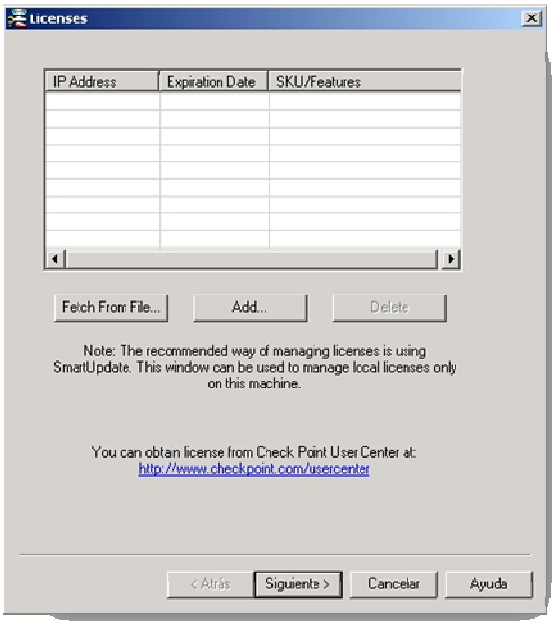


Gráfico 7

El Gráfico 8 muestra el punto de la instalación Check Point pide agregar los administradores del FireWall-1 con sus respectivos permisos. En el caso de no disponer de toda la información necesaria este paso se lo puede completar posteriormente.

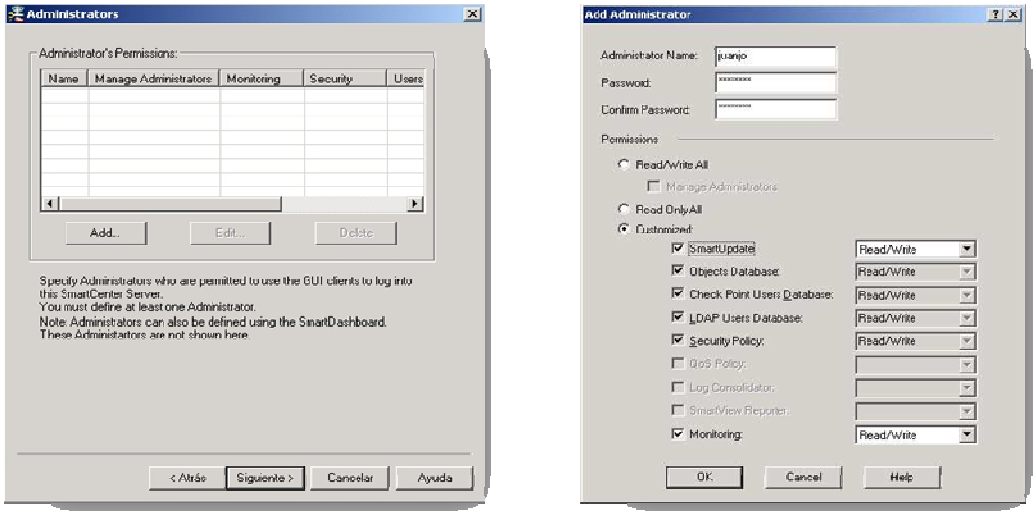


Gráfico 8

El Gráfico 9 muestra como se genera la semilla para operaciones criptográficas. Esto se produce a base del ingreso de caracteres randómicos hasta que la barra inferior indique que ha terminado el proceso.

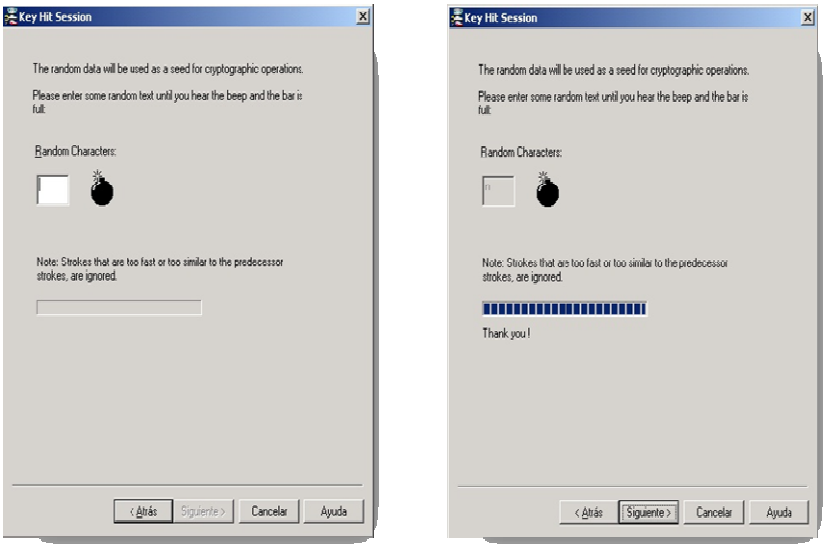


Gráfico 9

La consola de administración es la encargada de permitir la creación y la edición de las políticas de seguridad de la empresa. Existen tres aplicaciones que constituyen esta consola:

1. Editor de políticas: Permite ver y modificar las políticas de seguridad.
2. Indicador de Registros: Permite observar los registros del firewall.
3. Indicador de Estatus: Permite observar el estatus básico del sistema y despliega alertas del firewall.

Es importante aclarar que las cuentas administrativas que se van creando no tienen nada que ver con las cuentas del Sistema Operativo o cuentas creadas para autenticar otros servicios del firewall. El número de permisos y restricciones que se asignen a los usuarios varían según la versión del firewall y aumentarán aun más cuando haya nuevas versiones.

Una vez creada las cuentas administrativas, es necesario decirle a la consola administrativa qué dirección de red está autorizada para utilizar dichas cuentas. El archivo que guarda esta información, contiene una lista simple de una dirección de red o DNS del host por cada línea.

Únicamente puede haber un usuario a la vez utilizando el Editor de Políticas de Seguridad en modo de lectura y escritura. Esto está hecho así para poder prevenir que varios administradores de la plataforma escriban sobre los cambios y modificaciones de otro usuario. Si esto ocurre aparecerá un error indicando que existe otro administrador realizando modificaciones

Una regla base es una representación de una política de seguridad que determina quién, cuándo y qué puede realizarse[13]. En el editor de políticas de seguridad hay varios elementos que conforman esta política: objetos, reglas, anti intrusos y las propiedades de la política de seguridad en sí.

Se pueden crear varios objetos en el FireWall-1. Sin embargo los tres objetos principales son:

1. Objetos de red.

   Existen varios tipos de Objetos de Red que están diseñados para representar parte de la red corporativa y objetos de la consola de administración del FireWall-1. Estos objetos se los crea seleccionando el Menú Administración.

   - Estación de Trabajo: Este objeto representa una estación de trabajo individual dentro de la red.
   - Red: El objeto red se utiliza para representar una red o una subred.
   - Objeto Dominio**:** El objeto Dominio se utiliza para especificar un dominio DNS en particular.
   - Ruteador/Switch**:** El objeto ruteador o el objeto switch se utilizan únicamente cuando se desea administrar una lista de

[13] RATCLIFFE, Andrew*;* SHAH Inti; *Check Point VPN-1/FireWall-1 NG Administration;* Editorial McGraw Hill; 2002. pag.: 158

control en un ruteador o utilizar las opciones incluidas en el FireWall-1 para determinados switches, y es por esta razón que esta opción no se la toma en cuenta en la mayoría de casos.

- Grupo: Dentro de los objetos Grupo se pueden combinar varios objetos y llamarlos de una sola manera. Por ejemplo dos objetos de una misma red representan la red interna, por lo que a estos objetos se los puede agrupar dentro de un mismo objeto llamado red-interna.
- Rango de Direcciones**:** Los objetos de rango de direcciones se utiliza únicamente con el propósito de traducir direcciones de red.

2. Servicios

Firewall-1 de Check Point incluye cuatro tipos de grupos donde se encuentran servicios pertenecientes a estos. Estos grupos son:

1. TCP: protocolo de transmisión.
2. UDP: protocolo de datagrama de usuario.
3. RPC: llamada a procedimiento remoto.
4. ICMP: protocolo de mensajes de control y error de Internet.

Además de los servicios predeterminados, el administrador puede agregar elementos a estos grupos de servicios que no se encuentren en ninguna de las categorías mencionadas.

3. Tiempo

Estos objetos permiten que ciertas actividades se lleven a cabo en determinadas horas del día o en determinados días de una semana.

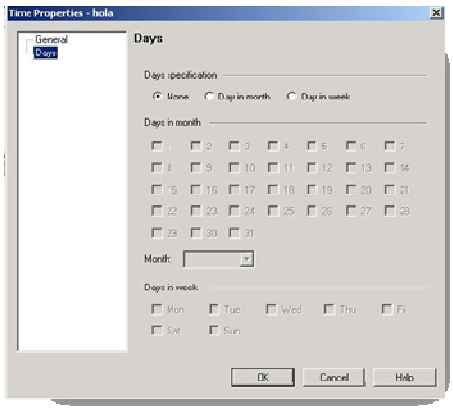


Gráfico 10

4. Políticas de seguridad y estándares implementados por Check Point aplicados en la tecnología VPN-1/FireWall-1

4.1 Análisis de la autenticación en un VPN-1

La autenticación a través del firewall brinda la garantía de que los usuarios pueden acceder a los servicios y sistemas de una manera segura para la infraestructura de las empresas. VPN-1/FireWall-1 puede realizar la autenticación de un usuario de la misma manera que lo realiza con objetos utilizando una dirección de red como fuente origen de la comunicación[14]. Existen tres tipos de autenticación que son validos: el usuario, el cliente y la sesión.

VPN-1 soporta diferentes tipos de esquemas de autenticación para administrar cuentas de usuarios tanto internas como externas a la organización:

- Clave Secreta: Este es un esquema que utiliza un sistema OTP (contraseña de una sola vez) con funciones criptográficas hash MD4 y MD5 y que está formado por tres partes: una contraseña numérica, una semilla (normalmente igual al nombre de usuario)

[14] RATCLIFFE, Andrew*;* SHAH Inti; *Check Point VPN-1/FireWall-1 NG Administration;* Editorial McGraw Hill; 2002. pag.: 239

y una clave secreta. La contraseña numérica y la semilla son transmitidas en forma de texto claro mientras que la clave secreta está codificada. Ingresando esta información se genera una respuesta que se utilizara de clave para la autenticación. Esta clave será siempre diferente y será válida únicamente si todos los datos ingresados también lo son. Existen varios sitios en el Internet de donde se pueden descargar generadores S/Key tales como:

- ftp://ftp.cs.sandia.gov/pub/firewall/skey/
- www.inner.net/pub/opie/
- www.phoneboy.com/sw/otpgen.zip
- ftp://ftp.tlogic.com/pub/skey
- http://reptile.rug.ac.be/~coder/sniffit/sniffit.html
- www.tlb.ch
- http://www.cs.umd.edu/~harry/jotp/

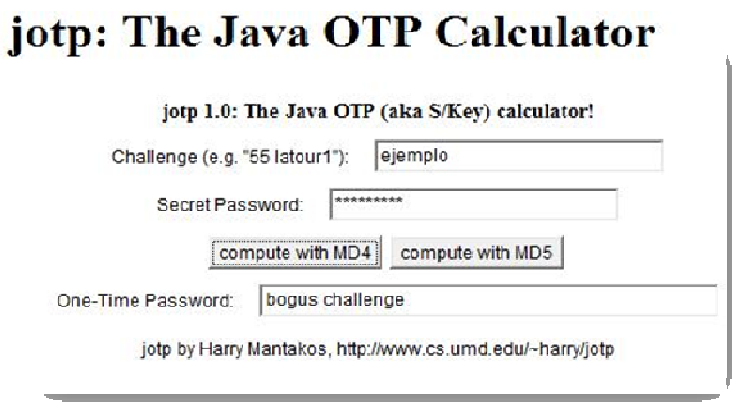


Gráfico 11

- Contraseña del Sistema Operativo: La VPN-1 de Check Point puede utilizar la contraseña del Sistema Operativo como esquema de autenticación. Con esto se limita la información que el SO provea en cuanto a cuentas de usuario y contraseñas que usualmente son claves estáticas de una longitud limitada. En este esquema no se utiliza ningún tipo de aplicación adicional.

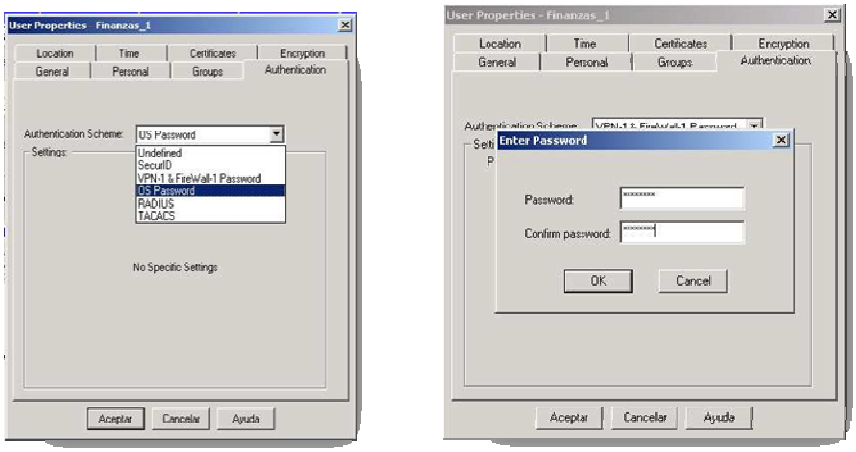


Gráfico 12

- Contraseña del FireWall-1/VPN-1: La contraseña del FireWall-1 es controlada internamente por el firewall. Esta puede ser máximo de ocho caracteres de longitud y es estática. En este esquema no se utiliza ningún tipo de aplicación adicional.

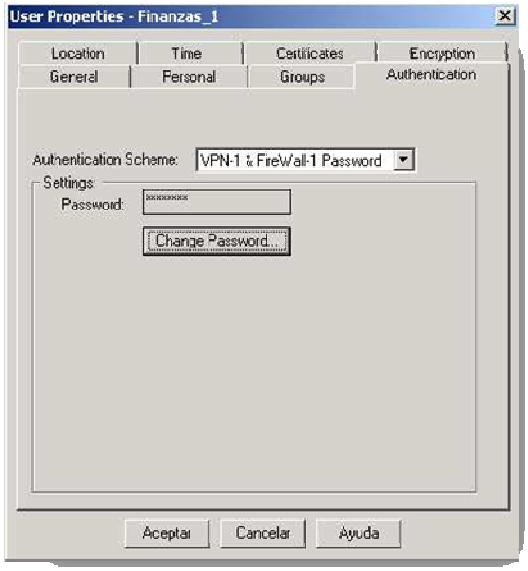


Gráfico 13

- Identidad Secreta: Este esquema de autenticación utilizan un generador físico que genera una identificación única y diferente aproximadamente cada minuto. Este generador esta sincronizado con un servidor que valida la autenticación por lo que mientras este generador no se pierda, la autenticación estará segura.

[15]

Gráfico 14

[15] http://www.easyfonds.info/english/Sicherheit_identifizierung.htm

Los usuarios pueden ser definidos con cualquiera de estos esquemas. Los usuarios pueden tener diferentes contraseñas en diferentes Gateways pero se puede tener un solo esquema de autenticación para todos los Gateways que estén bajo el mismo servidor de administración Firewall-/VPN-1.

La administración de usuarios y grupos para servicios de autenticación interna y externa requieren la creación de una planilla de usuario, un grupo y los usuarios que formaran parte del grupo. La planilla de usuario facilita y agilita la creación de usuarios ya que tiene como valores predeterminados las propiedades de los usuarios que van a ser creados.

Gráfico 15

Los usuarios individuales no pueden utilizarse directamente en una regla. Es por esto que se deben crear grupos de usuarios para poder establecer autenticación de usuarios.

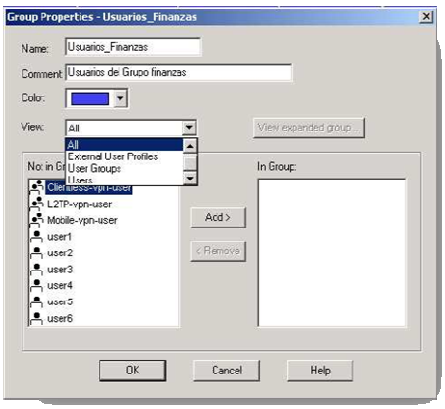


Gráfico 16

Una vez que se ha creado un grupo se puede empezar a agregar usuarios a este grupo. Si la plantilla fue creada correctamente únicamente se deberán ingresar las contraseñas para cada uno de los usuarios.

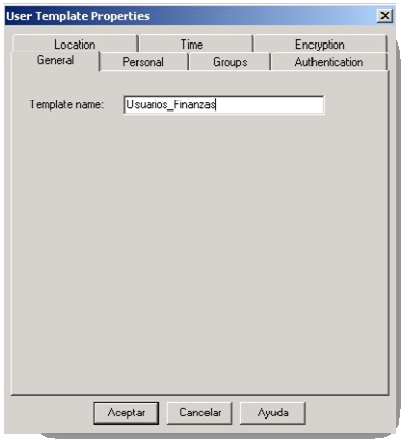


Gráfico 17

Gráfico 18

Una vez creados los usuarios se instalará la Base de Datos de Usuarios dentro de los módulos de FireWall-1/VPN-1. La autenticación de usuarios utiliza los Servidores se Seguridad de FireWall-1/VPN-1 donde autentica el usuario antes que se pueden comunicar con el dispositivo de destino. La autenticación de usuarios no requiere de ninguna aplicación adicional o procedimientos extras por parte del usuario. Los servicios que soporta el Sistema son HTTP, Telnet y FTP. La autenticación se la realiza una por conexión y es transparente para los usuarios.

Se debe tener especial cuidado con las reglas base ya que los servidores de seguridad de autenticación primero revisan si la conexión es permitida mediante la regla menos restrictiva. De existir

esta regla, se puede dar lugar a que exista conexión más no la autenticación.

Si se especifica un tiempo al usuario y uno a la regla, el usuario podrá utilizar la regla únicamente cuando los horarios de ambas opciones coincidan.

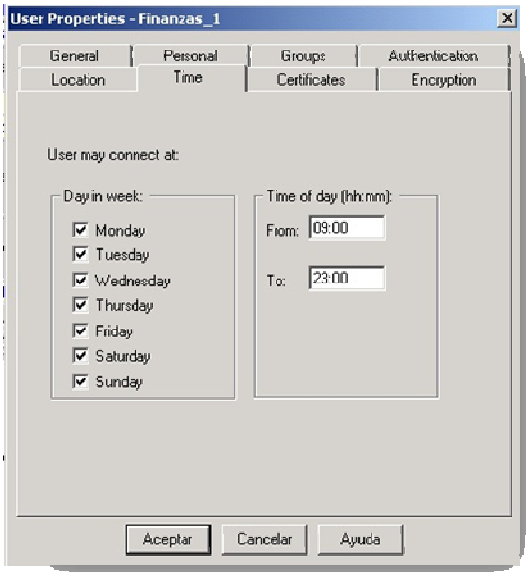


Gráfico 19

Existen varios métodos que son permitidos para el proceso de autenticación de usuarios. La propiedad marcada por defecto es manual. Los métodos se mencionan a continuación:

- Manual: El usuario tiene que iniciar la autenticación del cliente en el Gateway de una de las dos maneras siguientes:
  - Con un Telnet.

  - Por HTTP iniciando una sesión a través del navegador de internet. La dirección URL debe incluir el nombre del Gateway y el numero del puerto como por ejemplo:
    - http://gateway:900

- Parcialmente Automático: Si una conexión coincide con una regla, y el servicio es un servicio autenticado (Telnet, HTTP, FTP), el ingreso del usuario es aceptado después de una autenticación de usuario exitosa.
- Completamente Automático: Si una conexión que utiliza cualquier servicio coincide con una regla, el ingreso del usuario es aceptado luego de ser autenticado por el Agente de Autenticación de Sesión de FireWall-1/VPN-1. Si el servicio es un servicio autenticado, el ingreso del usuario será aceptado a través del mecanismo de autenticación de usuarios. Esta opción requiere que se instale el Agente de Autenticación de Sesión de FireWall-1/VPN-1 de lado del cliente.
- Agente de Aceptación de Ingreso Automático: Provee una autenticación del cliente de manera transparente. El ingreso de los usuarios es validado a través del Agente de Autenticación de Sesión de FireWall-1/VPN-1. Si la autenticación es exitosa, el acceso es garantizado desde la dirección de red la cual originó la conexión. Esta opción requiere que se instale el

Agente de Autenticación de Sesión de FireWall-1/VPN-1 en cada uno de los clientes.

- Ingreso Simple: El administrador de direcciones de Check Point provee un acceso de red transparente al usuario. En este método, FireWall-1/VPN-1 consulta en su base de datos la información de la dirección de red del usuario para determinar qué usuario se encuentra conectado en dicha dirección de red.

Gráfico 20

El proceso de autenticación comienza cuando el módulo de inspección se conecta al Agente de Autenticación de Sesión. Una vez realizada esta conexión, el Agente de Autenticación de Sesión requiere las credenciales de identificación del usuario. Si la autenticación es exitosa, entonces el módulo del FireWall-1 /VPN-1 permite que la conexión pase a través del Gateway. La Autenticación de Sesión se realiza una por conexión pero sin embargo requiere la instalación del Agente de Sesión en la máquina del cliente. Cabe

señalar que el Agente de Sesión es un utilitario que provee el FireWall-1/VPN-1 de Check Point.

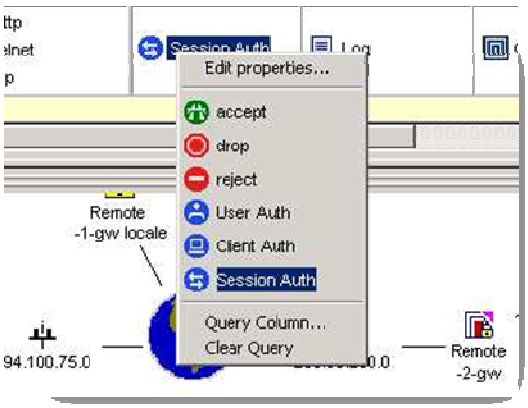


Gráfico 21

4.2 Análisis de la encriptación en un VPN-1

Encriptando las comunicaciones en redes públicas inseguras tales como el Internet, se puede utilizar FireWall-1/VPN-1 para construir Redes Privadas Virtuales sitio-a-sitio que proveen comunicaciones seguras entre dos participantes distintos. La privacidad, la autenticidad y la integridad de comunicaciones pueden ser encriptadas cifrando datos mientras que pasan a través de la red.

Tener buena seguridad implica una planificación muy cuidadosa de las políticas de seguridad que deben incluir controles de acceso y mecanismos de encriptación. Las estrategias y procedimientos de seguridad varían desde políticas simples de contraseñas hasta esquemas complejos de encriptación. El encriptar la información de

la compañía es un método muy importante de seguridad y provee uno de los servicios de seguridad más básicos en las redes de computación: intercambio de autenticación. Otros de los métodos que utilizan encriptación son las firmas digitales y la confidencialidad de información.

Cuando la información es enviada a través de una red pública tal como es el Internet, los mensajes pasan por medio de varios ruteadores, Gateways, y otros equipos internos de red hasta llegar a su destino final. Hay varios puntos donde la información puede ser interceptada o alterada o un falso mensaje puede ser enviado haciéndolo parecer que se origina desde un sitio confiable sin ser esto verdad. Para evitar cualquier pérdida o alteración de la información de la compañía se recomienda lo siguiente:

- Privacidad: Nadie más que los participantes de comunicación deben entender la comunicación.
- Integridad: Nadie ha interferido en la comunicación.
- Autenticidad: Nadie está enviando una comunicación falsa.

La autenticación de un mensaje verifica la autenticidad del remitente y del mensaje, comprobando que no exista filtración e interferencia en la comunicación.

La manera más simple de cifrar un mensaje es usando una clave secreta que cifre y descifre el mensaje. Asegurar la privacidad de la clave es crítico, puesto que cualquier persona que sepa la clave puede descifrar y leer el mensaje.

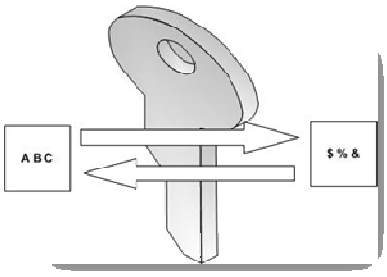


Gráfico 22

El cifrado de clave secreta es simple y rápido, pero hay dos problemas asociados a su uso:

- Se requiere un canal seguro por el cual los participantes puedan convenir en una clave antes de su primera comunicación cifrada. Una negociación directa puede ser ineficiente o irrealizable, y los participantes pueden tener que convenir en una clave por correo o por teléfono o algunos otros medios relativamente inseguros.
- El número de claves requeridas puede llegar a ser rápidamente inmanejable, puesto que debe haber una clave diferente para cada par de posibles participantes.

Los sistemas de claves públicas, donde cada participante tiene un par de claves, pueden solucionar estos dos problemas. Un par de claves se compone de dos claves matemáticamente relacionadas: una clave pública conocida por cada uno, y una clave privada conocida únicamente a su dueño

El sistema de distribución de claves públicas de Diffie-Hellman[16] se puede utilizar para compartir una clave secreta sin comunicar ninguna información secreta, por lo que no se requiere un canal seguro para el intercambio de claves. Bajo este sistema se requiere administrar únicamente un par de claves por cada participante en lugar de tener una clave para cada par de participantes. Una vez que los participantes hayan obtenido la clave secreta compartida, pueden utilizarla para cifrar comunicaciones entre ellos.

En contraste con un par de claves públicas y privadas de Diffie-Hellman, un par de claves públicas y privadas de RSA se utiliza para cifrar y descifrar mensajes. Un mensaje cifrado con la clave pública se puede descifrar solamente con la clave privada, y viceversa.

[16] RATCLIFFE, Andrew*;* SHAH Inti; *Check Point VPN-1/FireWall-1 NG Administration;* Editorial McGraw Hill; 2002. pa4.: 341

En el esquema del cifrado FWZ[17], los servidores de gestión de firewall funcionan como Autoridades Certificadoras para los Gateways de cifrado.

En el esquema del cifrado de ISAKMP, el PKI (Infraestructura de Claves Públicas) puede ser utilizado para obtener certificados para los Gateways de cifrado y para los usuarios de SecuRemote de Check Point.

Un esquema del cifrado consiste en los siguientes elementos:

1. Un algoritmo de encriptación para los mensajes cifrados.
2. Un algoritmo de la autenticación para asegurar la integridad de los mensajes y que estos no hayan sido interferidos.
3. Un protocolo de gestión de claves para generar e intercambiar claves.

La plataforma de Check Point, FireWall-1, soporta los siguientes esquemas de cifrado:

1. FWZ: este es un esquema de cifrado propio de FireWall-1.
2. IPSec manual: IPSec manual es un esquema de cifrado y autenticación que utiliza claves fijas.

[17] RATCLIFFE, Andrew*;* SHAH Inti; *Check Point VPN-1/FireWall-1 NG Administration;* Editorial McGraw Hill; 2002. pag.: 351

3. SKIP (Gestión de Claves Simples para Protocolos de): desarrollado por Sun Microsystems, agrega dos características al esquema de cifrado IPSec manual:
    a. Claves mejoradas: IPSec manual utiliza claves fijas mientras que SKIP utiliza una jerarquía de claves en constante cambio.
    b. Administración de claves: IPSec manual no proporciona un mecanismo por el cual los usuarios pueden intercambiar claves. SKIP implementa un protocolo de administración de claves para el esquema IPSec manual[18].
4. ISAKMP/OAKLEY (Asociación de Seguridad del Internet y Protocolo de Gestión de Claves) es un protocolo de intercambio de clave basado en el algoritmo Diffie-Hellman, pero que provee mayor seguridad. Es un protocolo genérico que no define formatos específicos al igual que SKIP, ISAKMP/OAKLEY, más conocido como ISAKMP, agrega la gestión de claves al esquema IPSec manual.

La relación entre los componentes de los esquemas de cifrado, según se los implementa en FireWall-1, se describe a continuación:

[18] WELCH –ALBERNATHY, Daemon*;* SHAH Inti; *Essential Checkpoint Firewall-1: An Installation, Configuration, and Troubleshooting Guide;* Pearson Education Inc.; 2002 pag.: 330

Esquema de cifrado	Algoritmo de autenticación	Algoritmo de Encriptación	La codificación se…
FWZ	MD5	DES, FWZ1	Se mantiene
IPsec Manual	MD5, SHA-1, CBC-DES MAC	DES, RC2	Se encapsula
SKIP	MD5, SHA-1, CBC-DES MAC	DES (triple DES para cifrado de claves) – El cifrado de tráfico es IPSec	Se encapsula
ISAKMP/OAKLEY	MD5, SHA-1	MD5, SHA-1	Se encapsula

Los algoritmos de cifrado DES, FWZ1, CAST, RC2, RC4 y RC5 son utilizados para cifrar la porción que contiene los datos de un paquete[19].

En el esquema del cifrado propio de FireWall-1 de Check Point, FWZ, el mensaje se cifra con una clave secreta derivada de una manera segura de las claves correspondientes de Diffie-Hellman.

[19] http://www.checkpoint.com/support/technical/online_ug/firewall-14.0/vpintro.htm#5307

Las claves de Diffie-Hellman son autenticadas por una Autoridad Certificadora.

Bajo este esquema, el número de claves que deben ser manejadas es proporcional al número de participantes. Esto es el contraste con algunos de los otros esquemas en los cuales el número de las claves que se manejan es proporcional al cuadrado del número de participantes.

Las aplicaciones encargadas de los protocolos hacen que las cabeceras del paquete TCP/IP no se cifren para que estos entreguen correctamente los paquetes. La cabecera de texto legible de TCP/IP se combina con la clave de sesión para cifrar la porción de los datos de cada paquete. Una suma de comprobación criptográfica se encaja en cada paquete para asegurar la integridad de sus datos. Con este proceso, la longitud del paquete no cambia, por lo que la UMT (unidad máxima de transmisión) sigue siendo válida.

IPSec manual es un esquema del cifrado y de autenticación[20]. IPsec también se puede configurar para conectar una red completa tal como una LAN o una WAN a una red remota a través de una

[20] WELCH –ALBERNATHY, Daemon*;* SHAH Inti; *Essential Checkpoint Firewall-1: An Installation, Configuration, and Troubleshooting Guide;* Pearson Education Inc.; 2002 pag.: 319

conexión red a red. Una conexión de red-a-red requiere la configuración de enrutadores IPsec en cada lado de las redes para procesar y enrutar la información de forma transparente desde un nodo en una LAN a otro nodo en una LAN remota. El Gráfico 1 muestra el nivel del modelo OSI en el que se ejecuta IPSec, siendo el mismo donde se ejecuta el módulo de inspección.

Teniendo dos LANs separadas por la Internet se deben utilizar enrutadores IPsec para autenticar e iniciar una conexión usando un túnel seguro a través de la Internet. Los paquetes que son interceptados en tránsito requerirán un descifrado de fuerza bruta para poder descifrar el código protegiendo los paquetes entre las LANs. El proceso de comunicación desde un nodo en dirección de una red a otra distinta es completamente transparente a los nodos puesto que el procesamiento encriptación/descifrado y el enrutamiento de los paquetes IPsec son manejados completamente por el enrutador IPsec.

Una Asociación de Seguridad (AS) se asocia a cada paquete, que consiste de:

- Funcionalidad: indica si el paquete está cifrado, autenticado, o ambos.

- Algoritmos: especifica el algoritmo del cifrado (como por ejemplo DES) y el algoritmo de autenticación (como por ejemplo MD5) usado en el paquete.
- Las claves utilizadas en los algoritmos.
- Datos adicionales como por ejemplo, el vector de inicialización (vi).

Un número de 32 bits, conocido como Índice de Parámetros de Seguridad (SPI), identifica una AS específica. Un SPI es simplemente un identificador, asignado por los mismos participantes con un significado particular dentro de su contexto, y no tiene ningún significado fuera de dicho contexto.

Los paquetes IP se cifran de acuerdo con el estándar de encapsulamiento de seguridad que provee autenticación, confidencialidad de datos e integridad del mensaje. El estándar ESP especifica que el paquete original es primero cifrado y después encapsulado en un paquete nuevo y más largo que el original. Existen dos modos de realizar esta encapsulación:

- Modo de Túnel
- Modo de Transportación

El modo de túnel es soportado por Firewall-1/VPN-1. El paquete entero (incluyendo la cabecera IP) se cifra de acuerdo con la

Asociación de Seguridad decidida previamente por los participantes. La cabecera ESP que contiene datos se agrega al principio del paquete, y así se crea una nueva cabecera IP. El paquete nuevo que es más grande que el paquete original consiste de:

- La nueva cabecera IP.
- La cabecera ESP.
- El paquete original cifrado.

La tabla a continuación presenta la comparación de los esquemas de cifrado soportados por la tecnología FireWall-1de Check Point[21].

Características	**FWZ**	**IPSec Manual**	**SKIP**	**ISAKMP/ OAKLEY**
Portabilidad	Propiedad de Check Point	Estándar de Mercado	Estándar soportado por Sun y otras tecnologías	Estándar de mercado
Gestión de Claves	Si	No	Si	Si
Claves de	Cada	Fijas	Cambian	Las claves

[21] http://www.checkpoint.com/support/technical/online_ug/firewall-14.0/vpintro.htm#5307

Sesión	sesión TCP o UDP tiene una nueva clave		en intervalos fijos, o cuando la cantidad de información cifrada excede un tamaño dado	se pueden modificar tan seguidas como sea necesario durante el tiempo que tenga una conexión
El número de claves requeridas es proporcional a...	Al número de participantes	Al cuadrado de del número de participantes	Al número de participantes	Al cuadrado de del número de participantes
Tamaño del paquete	No cambia	Crece	Crece	Crece
El Gateway puede	Si	Si (en modo	Si (en modo	Si (en modo

cifrar/descifrar en nombre de otros hosts		túnel)	túnel)	túnel)

4.3 Análisis de las políticas de seguridad utilizadas por VPN-1 /FireWall-1 de Check Point

Las pantallas de las propiedades de las políticas de seguridad, controlan gran parte de las Reglas Base. Es importante conocer lo que estas propiedades se refieren y como afectan a las reglas. Todas las reglas a crear tienen una de las tres siguientes maneras de presentarse:

- Primera Regla: Esta propiedad ubica a la regla creada en la primera posición antes de cualquier regla dentro del listado de las Reglas Base.
- Penúltima Regla: Esta propiedad ubica a la regla creada una posición antes de la última regla dentro del listado de las Reglas Base.
- Última Regla: Esta propiedad ubica a la regla creada en la última posición dentro del listado de las Reglas Base.

Las siguientes opciones son propiedades que se pueden aplicar a las reglas en Firewall-1/VPN-1.:

- Aplicar reglas de Gateway en la dirección de la Interfaz

- Aceptar respuestas UDP
- Habilitar descifrado al aceptar
- Aceptar control de conexiones VPN-1 y FireWall-1
- Aceptar RIP (protocolos de información de ruteo)
- Aceptar nombre de dominio sobre consultas UDP
- Aceptar nombre de dominio sobre zona de transferencia TCP
- Aceptar ICMP
- Aceptar paquetes de salida originados en el Gateway
- Registro de reglas Implícitas
- Instalar políticas de seguridad solamente si pueden ser instaladas satisfactoriamente en todos los destinos seleccionados

En lo que a servicios se refiere existen Firewall-1/VPN-1 presenta las siguientes opciones:

- Habilitar Conexiones de Datos por el Puerto FTP
- Habilitar Conexiones de Datos en Modo FTP Pasivo
- Habilitar Control RPC (Llamada a Procedimiento Remoto)

Las reglas deben ser creadas y posicionadas en el orden que se quiere que estas actúen. Cada regla tiene varios elementos que forman parte de ella:

- Origen y Destino
- Servicios

- Acción
    - Aceptar
    - Expulsar
    - Rechazar
    - Autenticación Sesión/Usuario/Cliente
- Rastreo
    - Sin guardar información
    - Almacenar información general
    - Almacenar información detallada
    - Almacenar acciones aceptadas
    - Alerta por Correo Electrónico/Alerta por SNMP (protocolo simple de administración de red)/descubrir al intruso
- Instalar
- Tiempo
- Comentario

A continuación, en el Gráfico 23[22], se puede observar con mayor claridad la aplicación de las reglas dentro de Firewall-/VPN-1 y el objetivo de las mismas en el proceso desde que entra un paquete hasta que sale o es rechazado por el firewall.

[22] WELCH –ALBERNATHY, Daemon*;* SHAH Inti; *Essential Checkpoint Firewall-1: An Installation, Configuration, and Troubleshooting Guide;* Pearson Education Inc.; 2002 pag.: 78

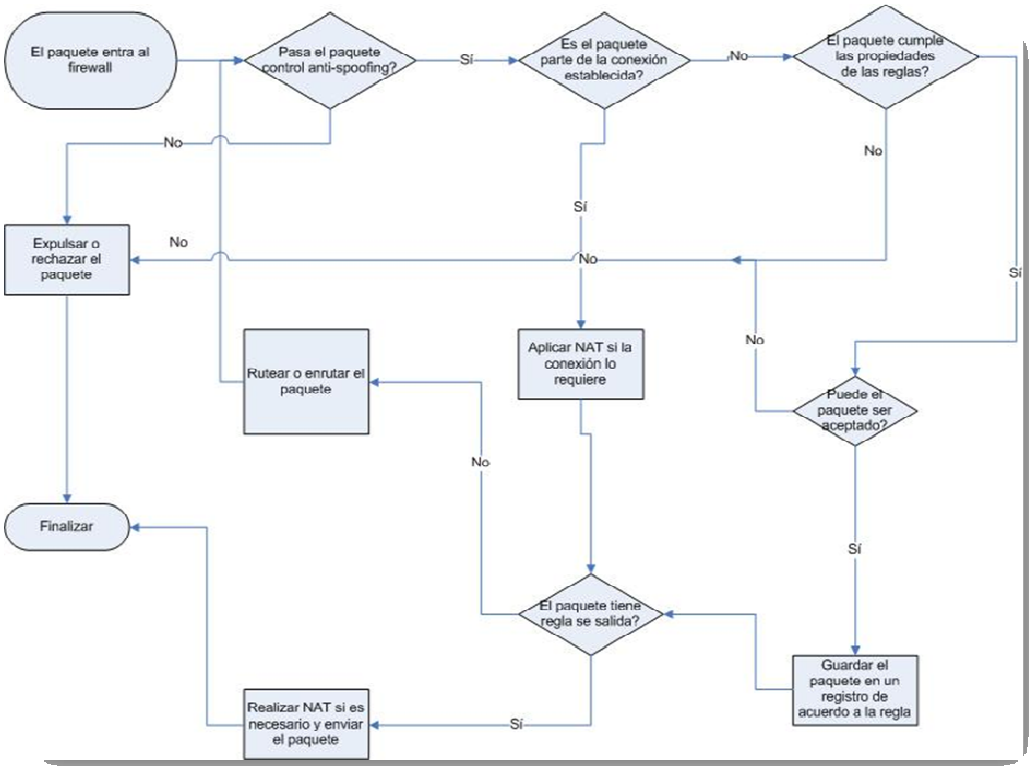


Gráfico 23

4.3.1 Ejemplo de Reglas Base

El ejemplo que se presenta a continuación muestra un ejemplo de red. Este se traduce a las reglas del firewall utilizando los siguientes elementos:

- Un objeto de red para la red 192.168.0.128/25, llamado red-192.168.0.128-25.
- Un objeto de red para la red 192.168.0.64/265, llamado red-192.168.0.64-26.

- Un objeto de grupo llamado red-interna que contiene a la red-192.168.0.128-25.
- Un objeto de grupo llamado red-DMZ que contiene la red-192.168.0.64-26.
- Un objeto tipo estación de trabajo para el servidor Web llamado servidor-Web.
- Un objeto tipo estación de trabajo para el servidor de correo llamado servidor-mail.
- Un objeto tipo estación de trabajo para la consola administrativa del firewall llamado firewall.

Utilizando esta red como ejemplo se generan las políticas de la empresa definidas a continuación:

1. Todos pueden acceder al servidor de correo vía SMTP. El acceso a este servicio no será guardado en un registro en el firewall.
2. Todos pueden acceder al servidor Web vía HTTP. El acceso a este servicio no será guardado en un registro en el firewall.
3. Las máquinas de la red interna 192.168.0.128/25 pueden acceder al servidor SMTP vía POP3. El acceso a este servicio será guardado en un registro corto en el firewall.

4. Las máquinas de la red interna pueden acceder al servidor HTTP vía SSH. El acceso a este servicio será guardado en un registro corto en el firewall.
5. Las máquinas de la red interna pueden acceder al Internet vía HTTP, HTTPS y FTP. El acceso a este servicio será guardado en un registro largo en el firewall.
6. A excepción de las reglas mencionadas, todo el tráfico restante debe ser rechazado. Todos los paquetes expulsados serán guardados en un registro largo en el firewall.

Estas regladas aplicadas en Firewall-1/VPN-1 se presentan en el Gráfico 24.

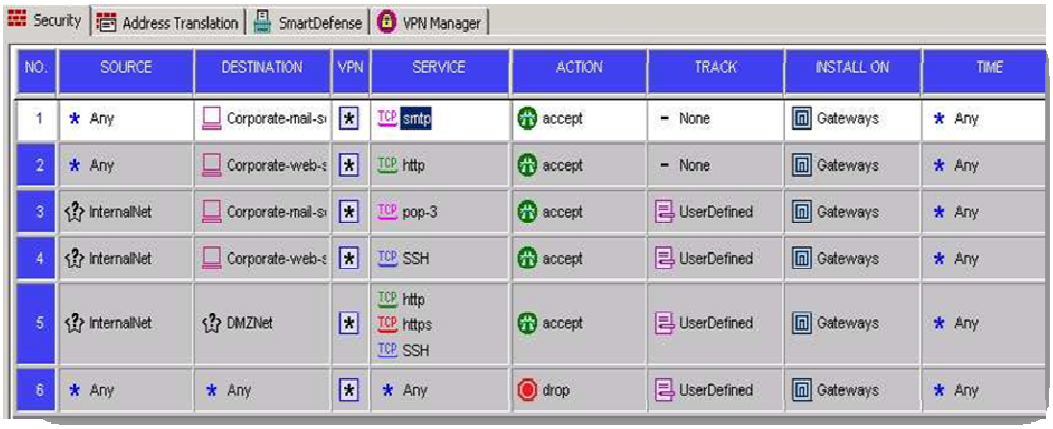


Gráfico 24

4.4 Estudio de los estándares de seguridad en un VPN-1/FireWall-1 de CheckPoint

Una vez realizado el estudio y el análisis de la manera en la que Check Point crea e instala las políticas de seguridad se debe estudiar quién realiza el complemento de este proceso llamado Seguridad Remota (*SecuRemote*) y Cliente Seguro (*SecureClient*). SecuRemote y Secure Client en realidad son dos nombres diferentes para la misma pieza de Software: Software para clientes de VPN para plataformás Windows. Este Software está diseñado para permitir a un usuario de Windows iniciar de manera transparente una conexión cliente-a-sitio VPN mediante un FireWall-1 de Check Point[23]. Resulta muy importante proporcionar el mismo tipo de seguridad tanto a clientes locales como a clientes móviles tales como personal de ventas que viajan o empleados que trabajan desde su casa. Los desafíos de ofrecer un acceso seguro a información confidencial requiere el ofrecer también políticas de seguridad a trabajadores móviles. Para poder cubrir las necesidades de estos usuarios, Check Point ha desarrollado conexiones de acceso remoto

[23] WELCH –ALBERNATHY, Daemon*;* SHAH Inti; *Essential Checkpoint Firewall-1: An Installation, Configuration, and Troubleshooting Guide;* Pearson Education Inc.; 2002 pag.: 365

mediante redes virtuales privadas y mediante clientes de acceso remoto.

SecuRemote y SecureClient proporcionan la aplicación del lado del cliente en una conexión VPN tipo cliente-a-sitio. Esta aplicación provee a los usuarios una conexión segura a los servicios remotos y además provee a los usuarios y administradores de la red de un nuevo modelo para el acceso remoto, substituyendo las costosas soluciones de marcado Dial-Up NAS/RAS, por un acceso remoto seguro, eficiente, flexible y de menor costo hacia las redes corporativas. Las aplicaciones SecuRemote y SecureClient pueden también ser utilizadas dentro de la red interna para proporcionar mayor seguridad para los sistemas críticos cifrando el tráfico dentro de dicha red.

Las aplicaciones SecuRemote y SecureClient de VPN-1 utilizan un sistema de encriptación de clientes. SecuRemote cifra la información antes de que esta abandone la máquina del usuario remoto proveyendo así seguridad para esta durante su tránsito. Debido a que SecuRemote y SecureClient trabajan a nivel de capa de red, no se necesita efectuar modificaciones en las aplicaciones del usuario. La integración de usuarios remotos es por lo tanto posible y trabajan como si estuvieran conectados con dentro de la red local.

Las aplicaciones para clientes remotos de Check Point son exactamente iguales a excepción de una sola cosa: SecureClient

apoya una política seguridad de escritorio que se hace parte del sistema del usuario. Esto amplía la tecnología Inspección de Estado de VPN-1/FireWall-1 hacia los usuarios dentro y fuera de la organización. Aunque toda la comunicación se cifra entre el cliente y la red de acceso remoto, la posibilidad existe para que el cliente este expuesto y para que la conexión VPN sea interceptada y utilizada de mala manera. La aplicación SecureClient elimina este riesgo totalmente permitiendo que el administrador controle y registre conexiones de entrada y de salida al escritorio de SecureClient.

La tabla a continuación muestra dónde es apropiado el uso de las aplicaciones SecuRemote y SecureClient[24]:

Propósito	**Uso de SecuRemote**	**Uso de SecureClient**
Acceso remoto seguro con una conexión a Internet de marcado vía MODEM	No se lo puede utilizar ya que el cliente puede ser atacado y el túnel ser interceptado	Si se lo puede utilizar ya que los usuarios portátiles tienen acceso a conexiones de marcado fácilmente y tienen un cliente protegido a través del Servidor de

[24] RATCLIFFE, Andrew*;* SHAH Inti; *Check Point VPN-1/FireWall-1 NG Administration;* Editorial McGraw Hill; 2002. pa4.: 379

		Políticas de Seguridad
Acceso a una red externa desde una organización conocida con una red corporativa protegida	Si se lo puede utilizar ya que el cliente ya se encuentra protegido dentro de la red de la organización conocida por lo que no se necesita proteger al cliente	Si se lo puede utilizar ya que en el caso de no poder verificar la seguridad de la red de la organización conocida, el cliente está protegido mientras esté conectado a su propia red externa
Acceso interno seguro a servidores	Si se lo puede utilizar ya que la protección de la información es suficiente en este caso	Si ya que si existe la posibilidad de que la seguridad del cliente se encuentre comprometida, no existe el riesgo de que tal cosa ocurra.
Acceso remoto seguro a Internet utilizando conexión de	Si le puede utilizar si la protección es brindada dentro del perímetro de la	Si ya que no se necesita ninguna seguridad extra dentro del perímetro de la

banda ancha	conexión del cliente	conexión del usuario para que esté seguro

Los administradores de VPN-1/FireWall-1 utilizan el editor de políticas de seguridad para la configuración de las aplicaciones SecuRemote y SecureClient. Este editor de políticas de seguridad se lo puede utilizar para controlar el acceso una vez establecida una conexión VPN cliente-a-sitio aplicando características tales como autenticación, registros y alertas utilizando conexiones descifradas.

La aplicación SecureServer VPN-1/FireWall-1 de Check Point es una versión diseñada para proteger un servidor de una sola aplicación. Esta aplicación provee control de acceso, autenticación del cliente y de la sesión, conversión de dirección de red (NAT), control de ingresos y auditoría para un solo host.

El protocolo SSL no protege los sistemas ni las aplicaciones, sino que permite la autenticación de servidores, la codificación de datos y la integridad de los mensajes. El protocolo SSL no difiere de una aplicación VPN de la capa de red, como lo hace IPSec y FWZ en las VPN de Check Point, aunque tiene pros y contras específicos. La ventaja principal del protocolo SSL es que este se instala conjuntamente cuando el navegador es instalado, en contrario a la instalación de SecuRemote que se lo hace después y esto puede causar algunas modificaciones en la configuración inicial del

navegador. La desventaja sin embargo, es que el protocolo SSL es un servicio específico, y no es especialmente escalable ni eficiente. No se lo puede aplicar en servicios UDP y las aplicaciones no SSL TCP no lo pueden utilizar.

La aplicación SecureServer también protege el servidor contra accesos no autorizados a la red, algo que el protocolo SSL no lo puede hacer. Los paquetes de las intercepciones de SecureServer intercepta paquetes por debajo del modelo IP y permite el acceso a políticas de seguridad complejas que los usuarios y las direcciones de red utilizan (SecureServer soporta la autenticación de clientes y sesiones), así como la protección contra diferentes clases de ataques tales como la negación de servicio, y la explotación de servicios no autorizados. Usando la aplicación SecureClient conjuntamente con SecureServer proporciona un método que permite desplegar los grupos de trabajo para usuarios locales remotos, algo que el protocolo SSL se encuentra lejos de poder proporcionar[25].

Los dos sistemas de cifrado, tanto IKE y como FWZ, varían en sus propiedades, capacidad y fuerza el momento de proveer encriptación. El sistema IKE siempre encapsula el paquete, es decir que lo cifra y crea una nueva envoltura para el paquete de datos original, permitiendo que los paquetes sean enrutados a través del

[25] http://www.checkpoint.com/support/technical/online_ug/firewall-14.0/vpsecure.htm#7342

Internet, inclusive si las direcciones de origen y destino son privadas. Se puede habilitar también la opción de Encapsular Conexiones para SecuRemote dentro de las opciones de FWZ. Si esto no se lo hace, se puede utilizar únicamente FWZ donde las direcciones pueden ser enrutadas, donde una parte del paquete es cifrado, a excepción de las direcciones originales de origen y de destino que permanecen con el valor del paquete de datos original[26].

IKE puede utilizar los sistemas AES (Estándar Avanzado de Cifrado, 256 bits), 3DES (Sistema Estándar de Cifrado, 168) y DES (56 bits). FWZ soporta FWZ1 (algoritmo de cifrado propiedad de Check Point que soporta claves con longitud de 40 bits) y DES.

Todos los métodos de autenticación soportados por el Gateway pueden ser utilizados por FWZ, pero IKE solo puede utilizar la contraseña de VPN-1/FireWall-1 como clave compartida. Sin embargo Check Point ha creado una extensión de IKE que acepta utilizar todos los métodos de autenticación: IKE híbrido.

El esquema IKE híbrido es una extensión del esquema IKE el cual soporta todos los métodos de autenticación de FireWall-1 tales como Tarjetas SecureID, RADIUS, LDAP o la contraseña interna de VPN-1/FireWall-1. Este esquema permite a los administradores de seguridad utilizar dos factores de autenticación muy poderosos para las conexiones de acceso remoto. Esto es muy favorable ya que

[26] http://www.tks.buffalo.edu/dir_office/mainop/secuRemote/UBREADME.html

limita los riesgos de que alguien pueda ingresar de manera indebida al sistema interno pudiendo adivinar cuentas de usuario y contraseñas.

Una vez instalada, dentro de los programás de Windows aparece la aplicación bajo el nombre de Check Point VPN-1 SecuRemote o SecureClient, donde se deben definir el nombre del servidor y su ubicación y configurar parámetros generales.

5 Prototipo de la red virtual (VPN-1) /FireWall-1 de CheckPoint en el Grupo MDM

5.1 Diseño de VPN-1/FireWall-1 de Check Point implementado por el Grupo MDM

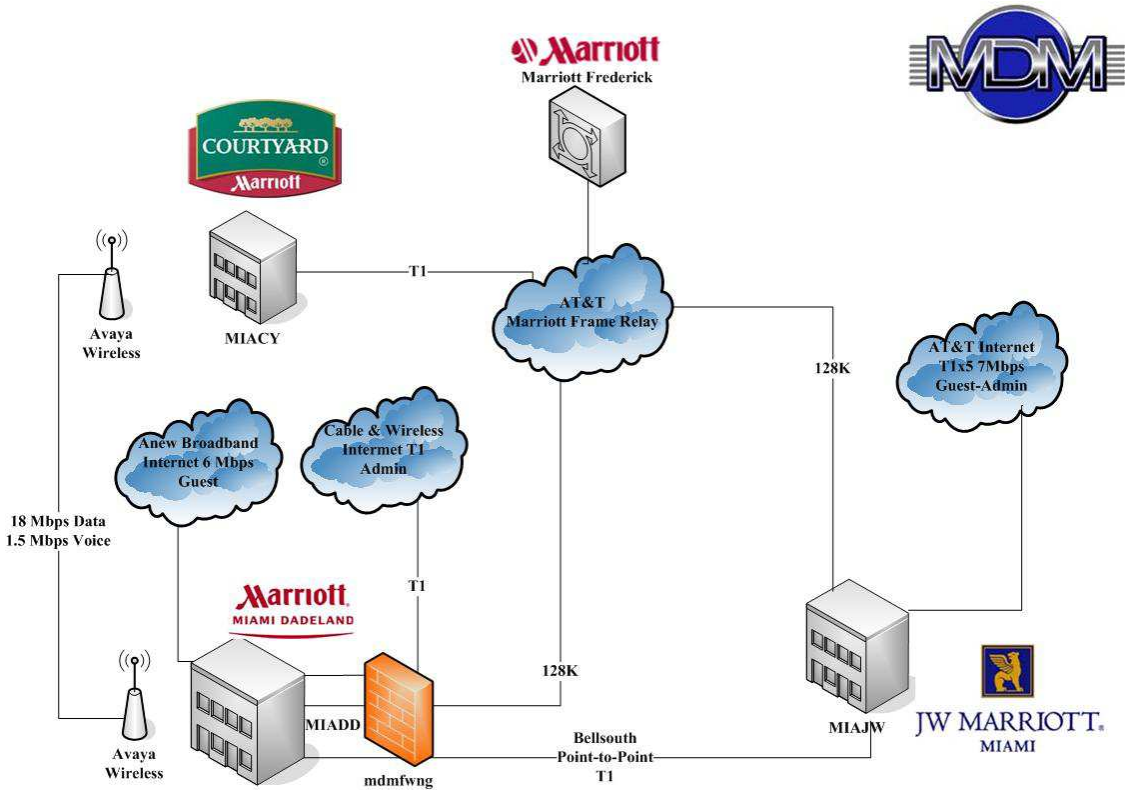


Gráfico 25

Con este diseño presentado en el Gráfico 25 para la implementación del firewall en el Grupo MDM, se intenta lograr una independencia de la corporación Marriott y hacer que esta participe únicamente en la administración de sus servidores más no en la parte operativa de las

tres propiedades JW Marriott, Miami Dadeland Marriott y Courtyard Dadeland by Marriott. Con esta independencia, será el Grupo MDM quien cree sus propias redes, administre sus usuarios e imponga sus políticas y sobretodo contar con una herramienta que las haga cumplir. Cabe resaltar que el firewall mdmfwg actúa sobre la parte administrativa de las propiedades más no sobre la red sobre la cual interactúan los huéspedes de las tres propiedades. Esto se da así ya que no se pueden bloquear puertos específicos que los huéspedes requieren para conectarse a sus oficinas remotas, muchos de los cuales no son los mismos que requieren los usuarios administrativos del Grupo MDM local y remotamente.

Siguiendo con el estándar del Grupo MDM, se buscó una tecnología que trabaje de manera segura sobre plataformás Windows, que sea fácil de administrar, que cuente con módulos gráficos y sencillos de entender, que se cuente con soporte técnico y sobretodo que sea amigable y transparente a los usuarios finales. Con la utilización Firewall-1/VPN-1 de Check Point se logra enrutar paquetes de manera segura sobre el Internet utilizando la herramienta de mayor protección seguridad sobre el Internet. El módulo de administración se pretende que este instalado físicamente en la propiedad principal MIADD, quien tendrá una conexión punto a punto con la propiedad MIAJW y una conexión inalámbrica con la propiedad MIACY.

5.2 Arquitectura de VPN-1/FireWall-1 de Check Point implementado por el Grupo MDM

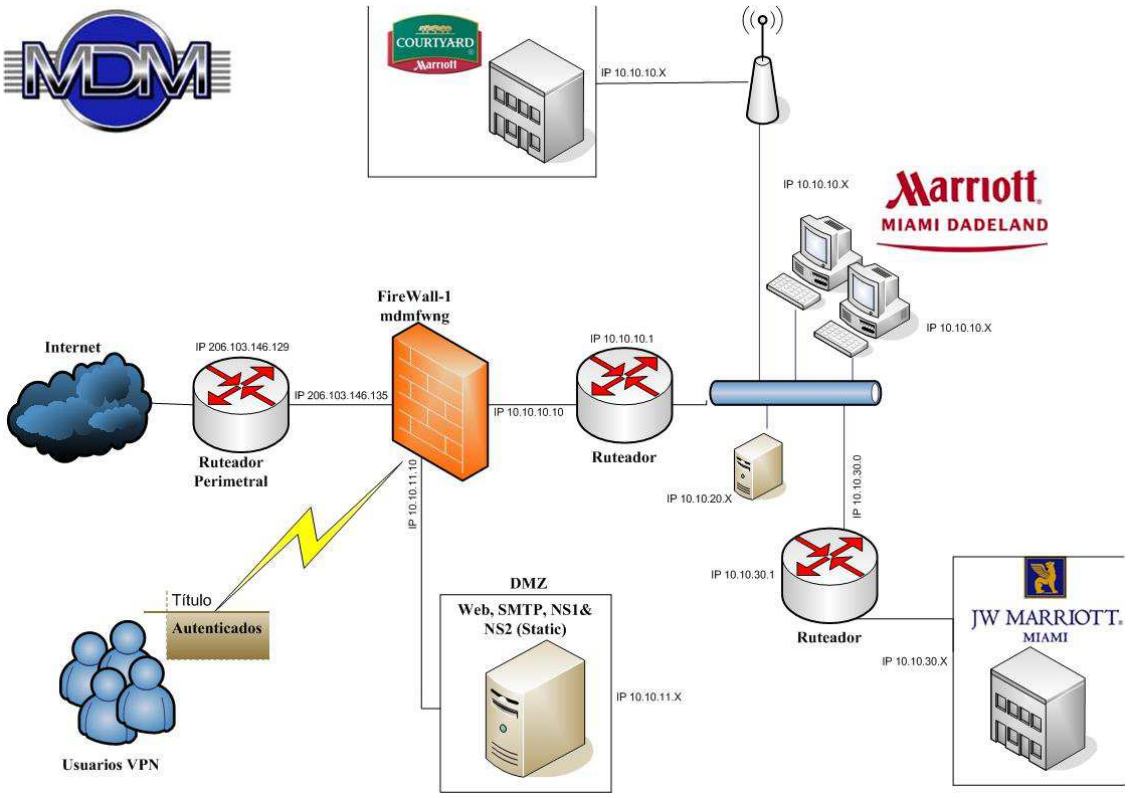


Gráfico 26

En el Gráfico 26 se presenta la arquitectura de la implementación del Firewall-1 “mdmfwng”[27]. Con la implementación de este firewall se logra cumplir el objetivo de independencia de la corporación Marriott en lo que a control de redes y servidores se refiere, y la relación queda limitada al control exclusivo de los servidores que dicha corporación debe tener en cada una de sus propiedades. Sin

[27] Nombre otorgado al Firewall-1 NG del Grupo MDM.

embargo, la parte administrativa del Grupo MDM queda en absoluto control del Grupo MDM y bajo la seguridad que ofrece la aplicación Firewall-1/VPN-1 de Check Point.

El ruteador perimetral es el ruteador principal contiene un dirección exterior del rango 206.103.146.x. Este ruteador se encarga de comunicarse con el Firewall-1 mdmfwng por medio de la tarjeta de red externa de dicho firewall. Un vez que el firewall reciba los paquetes que ingresan hasta el mismo, y luego de hacer cumplir las reglas establecidas por el Grupo MDM, asigna estos paquetes hacia su destino final ya sea pasando a través de otro ruteador interno o ingresando a la red DMZ done se encuentran ubicados bajo el rango de red 10.10.11.x los servidores de correo electrónico, servidores de Internet y servidores NS1 y NS2 estáticos. Si los paquetes están dirigidos hacia usuarios administrativos de la red 10.10.10.x, estos deben pasar a través del ruteador interno con dirección 10.10.10.1 que es el responsable de destinar los paquetes ya sea dentro de la red de la propiedad MIADD, hacia la propiedad MIACY que se encuentra en el mismo rango de red, hacia servidores específicos internos dentro de la red 10.10.20.x, o hacia un nuevo ruteador con dirección 10.10.30.1, que será el encargado de enrutar paquetes hacia los usuarios de la red 10.10.30.x. Para los paquetes de salida del Grupo MDM hacia el Internet, el proceso será idéntico

más en sentido contrario, ya que nada que este bajo la administración del Grupo MDM puede salir o entrar al mismo a no ser por medio del Firewall-1 mdmfwng.

Para los usuarios remotos que utilizan VPN-1 de Check Point existe un proceso de autenticación que consiste de un nombre de usuario y una contraseña almacenados dentro del firewall para cada usuario, que una vez que estos datos sean autenticados, podrán acceder a las redes a las cuales bajo las cuales están autorizados a trabajar de manera remota.

5.3 Políticas de seguridad utilizadas por el Grupo MDM

Dentro del Grupo MDM se manejan estándares y políticas asociadas con el uso del Internet y de correo electrónico. Estos estándares y políticas están descritos en el Libro del Asociado y en un documento el cual todo empleado debe firmar y comprometerse a cumplirlo haciéndose responsable por sus actos y las descritas consecuencias en caso de no hacerlo.

El texto original se encuentra desarrollado en ingles por lo que a continuación se presenta una traducción del mismo[28]:

Acceso al Internet

[28] Associate Handbook; ServingMiami Dadeland Marriott, JW Marriot Miami y Courtyard Dadeland by Marriott. Agosto 2006

“El acceso al Internet a través de MG Hospitality Group, Inc es un privilegio y conlleva responsabilidad que refleja uso responsable y ético del mismo. Se prohíbe a los usuarios/asociados tener acceso al Internet para uso personal en acciones tales como observar páginas Web con acceso a cuentas personales de correo electrónico, páginas Web personales, etc. y/o cualesquier propósito poco ético, incluyendo pornografía, violencia, apuestas, racismo, hostigamiento o cualesquier otra actividad considerada ilegal. Los asociados deben recordar que el uso de cualquier objeto de propiedad de MG Hospitality Group, Inc debe ser con el único fin de negocio de la propia compañía MG Hospitality Group, Inc. En cualquier momento y sin previo aviso ni anticipación del mismo, la gerencia se reserva el derecho de examinar cuentas de correo electrónico de la compañía, archivos y directorios personales, y demás información almacenada en las computadoras de propiedad de MG Hospitality Group, Inc. Los asociados no pueden asumir el derecho a la privacidad al usar computadoras, el Internet, el hardware o el software bajo licencia y propiedad adquirida por MG Hospitality Group, Inc, dentro de las instalaciones en donde MG Hospitality Group, Inc emplea a sus asociados. El uso del Internet por parte de los asociados constituye la aceptación de tal supervisión y monitoreo. Los asociados quienes fueran encontrados utilizando el Internet para uso personal trabajando y/o observando páginas Web con material no relacionado

e inadecuado al negocio de MG Hospitality Group, Inc es consideran una violación a las políticas de la compañía y estará conforme a la acción disciplinaria pudiendo llegar hasta la terminación del empleo".

La compañía MG Hospitality Group, Inc. ha establecido una política con el propósito de alcanzar el éxito donde se describe el acceso de los mensajes del correo electrónico creados, enviados, o recibidos por los asociados utilizando el sistema del correo electrónico de la compañía.

La compañía se propone honrar las políticas descritas a continuación, pero se reserva el derecho de cambiarlas en cualquier momento si las circunstancias así lo requieren.

1. La compañía posee y administra un sistema de correo electrónico. Este sistema es proveído por la compañía con el propósito de apoyar a la compañía ha desenvolverse en las reglas del negocio.

2. El hardware del sistema de correo electrónico es propiedad de la compañía. Adicionalmente, todo mensaje creado, enviado o recibido por el sistema de correo electrónico son y permanecerán bajo propiedad de la compañía. Estos mensajes no son propiedad de los asociados.

3. El uso del sistema de correo electrónico está enteramente relacionado entre la compañía y las reglas del negocio. El sistema no debe ser utilizado para negocios y uso personal.

4. El sistema de correo electrónico debe ser utilizado de acuerdo con la descripción laboral de cada uno de los asociados. Siendo consistentes con la política de no-solicitación, el sistema de correo electrónico no puede ser utilizado para uso comercial o con fines de solicitar algún servicio ajeno a las reglas del negocio de la compañía.

5. El sistema de correo electrónico no se puede utilizar de ninguna manera que sea contraria a las políticas de MG Hospitality Group, Inc. incluyendo la política de EOO que prohíbe el hostigamiento. El sistema del correo electrónico no debe ser utilizado para crear mensajes ofensivos o que vayan en contra de la compañía. Entre éstos que se consideren ofensivos está cualquier mensaje que contengan implicaciones sexuales, discriminaciones raciales, comentarios acerca de algún género en específico o cualesquiera otro comentarios que ofendan refiriéndose a la edad de una persona, orientación sexual, creencia religiosa o política, origen étnico o incapacidad.

6. El sistema del correo electrónico no será utilizado para enviar (subir) o para recibir (descargar) materiales con copia protegida, secretos comerciales, información financiera de la propiedad, o materiales similares sin la autorización previa.

7. La compañía se reserva y ejercita los derechos de ver, auditar, interceptar, y tener acceso a todos los mensajes eliminados, recibidos, o enviados desde el sistema del correo electrónico para cualquier propósito. El contenido de un correo electrónico obtenido correctamente para los propósitos legítimos del negocio se puede divulgar dentro de la compañía sin el permiso del asociado.

8. La confidencialidad de cualquier mensaje no debe ser asumida. Aun cuando un mensaje se borra, sigue siendo posible recuperarlo y leerlo. Además, el uso de contraseñas para seguridad no garantiza confidencialidad. Todas las contraseñas se deben divulgar a la compañía, caso contrario son inválidas y no pueden ser utilizadas.

9. A pesar que la compañía MG Hospitality Group, Inc. se reserva el derecho de recuperar y de leer cualquier mensaje de correo electrónico, todos los mensajes se deben tratar con carácter de confidencial por otros asociados y tener acceso a

ellos solamente por el destinatario previsto. No se autoriza a los asociados a recuperar o leer ningún mensaje de correo electrónico que no sane enviados al mismo. Cualquier excepción a esta política de seguridad debe recibir la aprobación previa del empleador.

10. Los asociados no utilizarán códigos, no tendrán acceso a un archivo, ni recuperarán ninguna información almacenada, a menos que estén autorizados para hacerlo. Los asociados no deben procurar acceder a mensajes de otros asociados sin el permiso de este último. Todas las contraseñas de computadora deben ser proporcionadas a los supervisores. Ninguna contraseña que no sea conocida por la compañía puede ser utilizada.

11. Cualquier asociado que descubra una violación de estas políticas de seguridad deberá notificará a Director de Recursos Humanos.

12. Cualquier asociado que viole estas políticas de seguridad o utilice el sistema del correo electrónico con propósitos incorrectos estará sujeto a la acción disciplinaria pertinente, incluyendo la terminación del empleo.

Políticas de Seguridad básicas a ser aplicadas en el Firewall-1 de Check Point del Grupo MDM

1. Realizar una regla de limpieza de Broadcast.
2. Los usuarios remotos VPN pueden conectarse a la red autorizada.
3. Los usuarios autorizados de la red VPN pueden conectarse a la red donde se encuentran los servidores administrativos.
4. Se permite el tráfico desde cualquier origen hacia el FireWall-1 únicamente después de realizada la autenticación de los usuarios.
5. Se permite el tráfico desde cualquier origen a los servidores DNS utilizando únicamente los servicios DNS, http, consultas al dominio vía UDP (*Domain Name System Queries*) y autenticación de clientes.
6. Se permite el tráfico desde los servidores DNS hacia cualquier sitio utilizando únicamente los servicios DNS, http y consultas al dominio vía UDP.
7. Se permite el tráfico desde cualquier sitio hacia los servidores de correo electrónico únicamente utilizando los servicios para correo electrónico (smtp, pop3, imap), http, https y DNS.
8. Se permite el tráfico desde los servidores de correo electrónico hacia cualquier sitio únicamente utilizando los

servicios para correo electrónico (smtp, pop3, imap), http, https y DNS.

9. Se permite el tráfico desde cualquier sitio hacia el servidor Web únicamente utilizando los servicios http y https.
10. No se permite el tráfico desde cualquier sitio hacia las redes internas utilizando servicios considerados troyanos, spyware o spams, utilidades del sistema de mensajería instantáneas utilizando audio y video ni nada que permita distribución de contenidos multimedia en la red.
11. Se permite el tráfico desde cualquier sitio hacia el servidor smtp únicamente utilizando los servicios smtp.
12. Se permite el tráfico desde el servidor smtp hacia cualquier sitio únicamente utilizando los servicios smtp.
13. Se permite el tráfico desde las redes VPN hacia cualquier sitio.
14. Se permite el tráfico desde cualquier sitio hacia los servidores XETA únicamente utilizando los servicios http.
15. No se permite tráfico alguno utilizando los servicios smtp, servicios considerados troyanos, spyware o spams, utilidades del sistema de mensajería instantáneas utilizando audio y video ni nada que permita distribución de contenidos multimedia en la red así como ningún directorio Napster.

16. Se permite el tráfico desde las redes internas y DMZ hacia cualquier sitio.
17. Realizar una regla de limpieza (*clean-up rule*).

Servicios y grupo de Servicios dentro de FireWall-1 de Check Point a utilizarse.

1. La regla de limpieza de Broadcast incluye los siguientes servicios:

   Estos servicios se muestran en los gráficos 27 y 28: Bootp, Rip y NBT.

Gráfico 27

Gráfico 28

2. Consultas al dominio vía UDP (*Domain Name System Queries*):

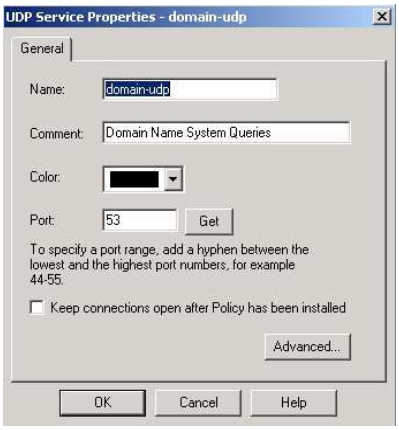


Gráfico 29

3. Imap: Protocolo de red de acceso a mensajes electrónicos almacenados en un servidor.

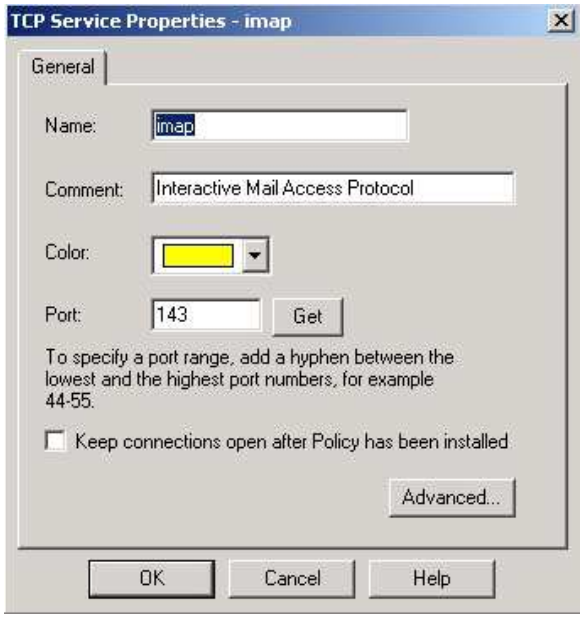


Gráfico 30

4. Servicios troyanos: Todos los servicios troyanos detectados se muestran en los gráficos 31 y 32.

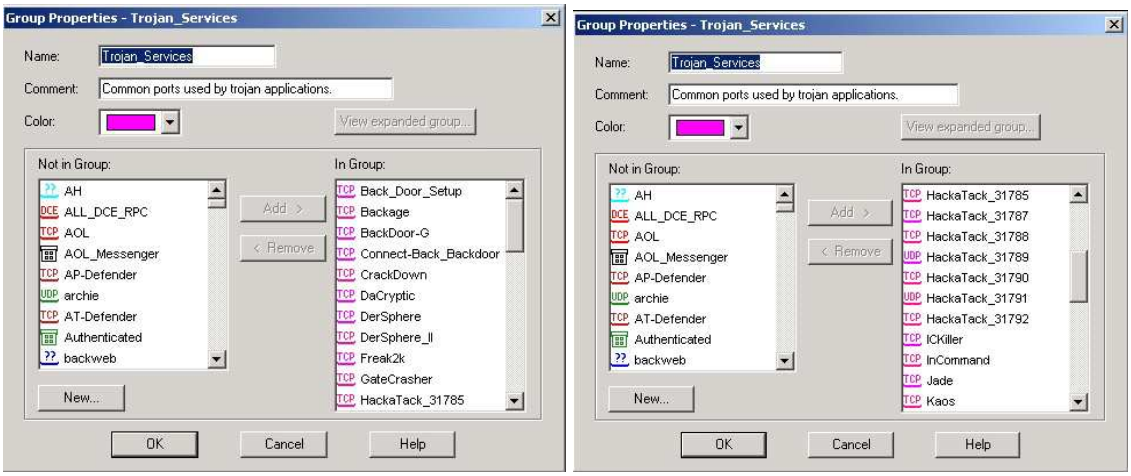


Gráfico 31

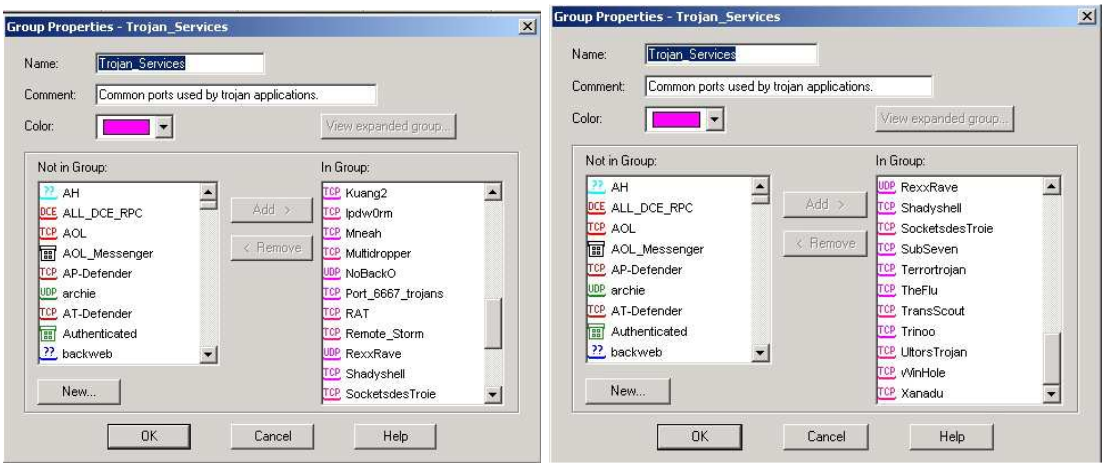


Gráfico 32

5. Servicios spyware y spam:

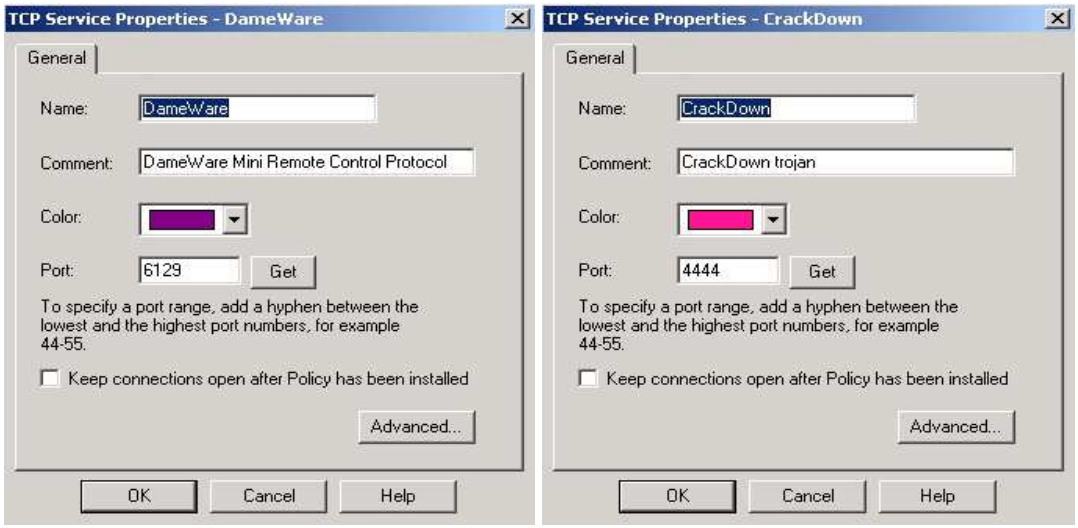


Gráfico 33

6. Servicios del sistema de mensajería instantáneas que utilizan audio y video:

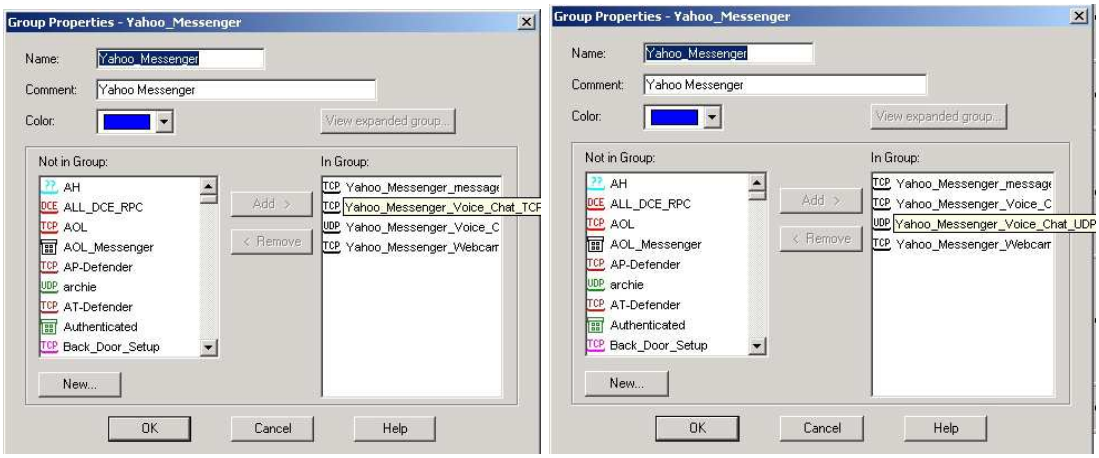


Gráfico 34

7. Servicios que permiten distribución de contenidos multimedia en la red:

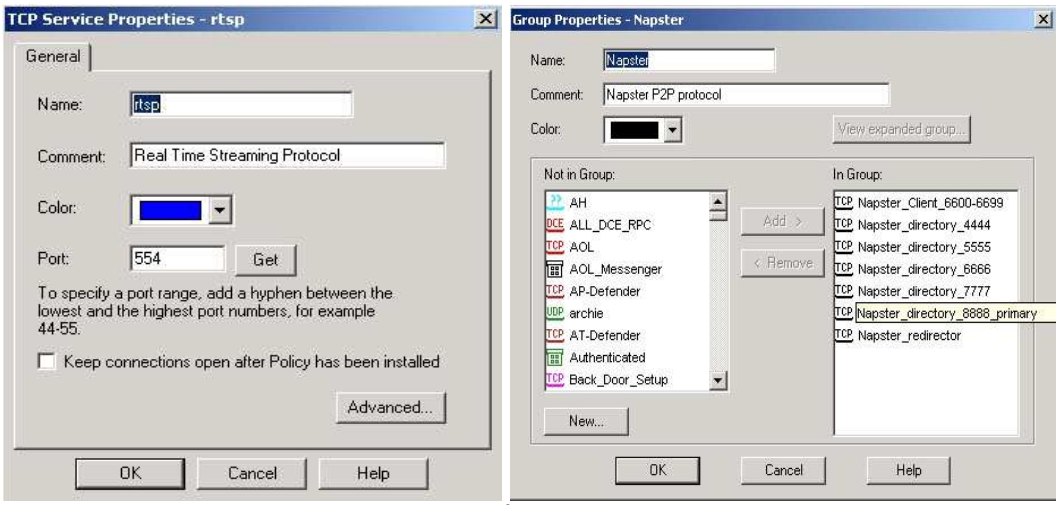


Gráfico 35

5.4 Implementación del Prototipo

Propiedades del FireWall-1 de Check Point mdmfwng:

Direcciones de las tarjetas de red del FireWall-1 mdmfwng.

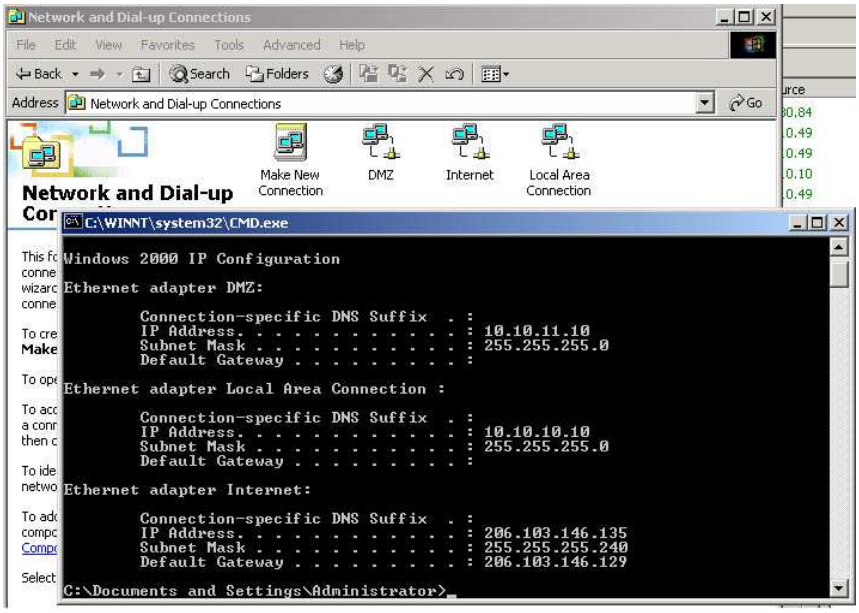


Gráfico 36

Ingreso de usuario y contraseña.

Gráfico 37

Ingreso de las licencias de Firewall-1/VPN-1

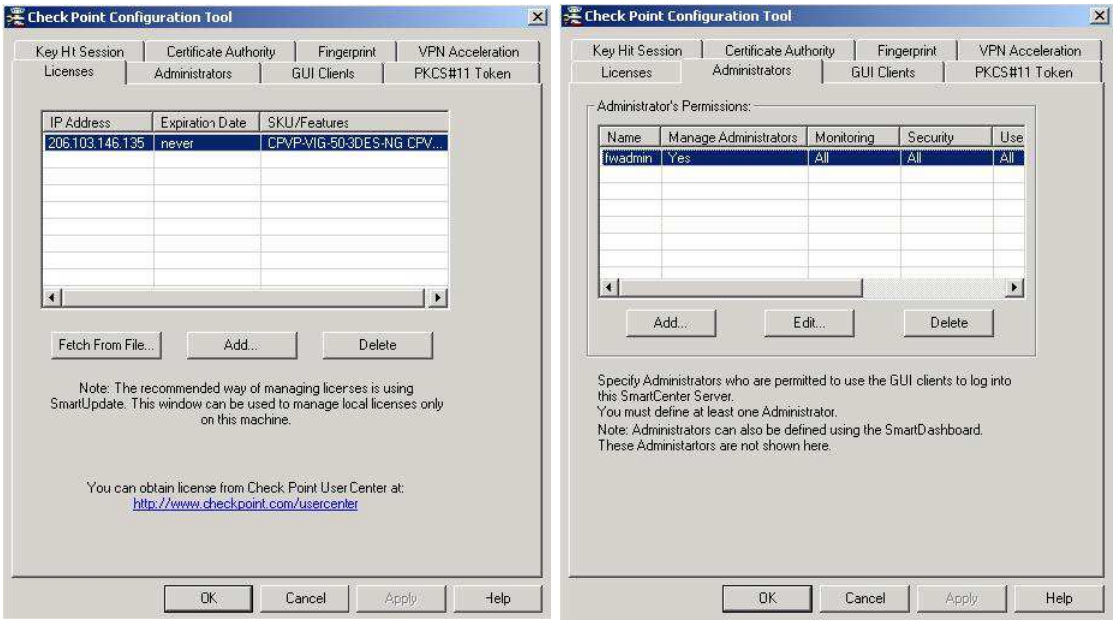


Gráfico 38

Direcciones de red que pueden acceder al Firewall.

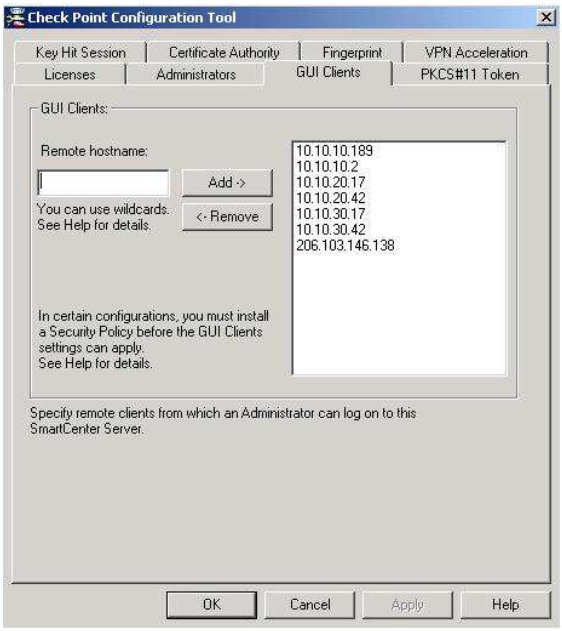


Gráfico 39

Nombre del Firewall (Autoridad Certificadora).

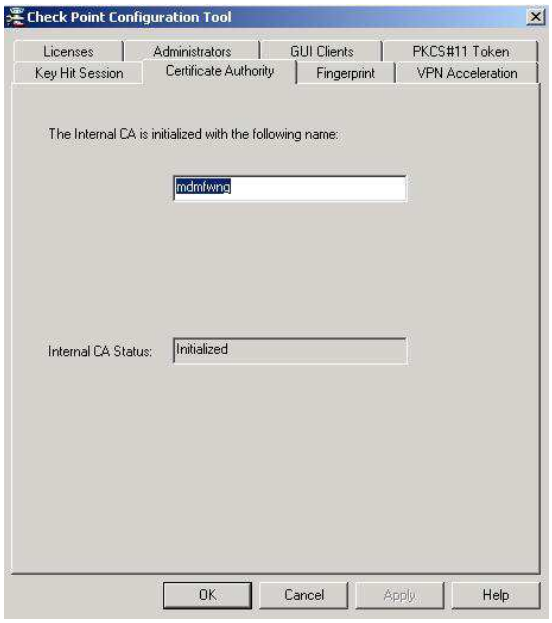


Gráfico 40

Propiedades del Objeto de Red Check Point mdmfwng

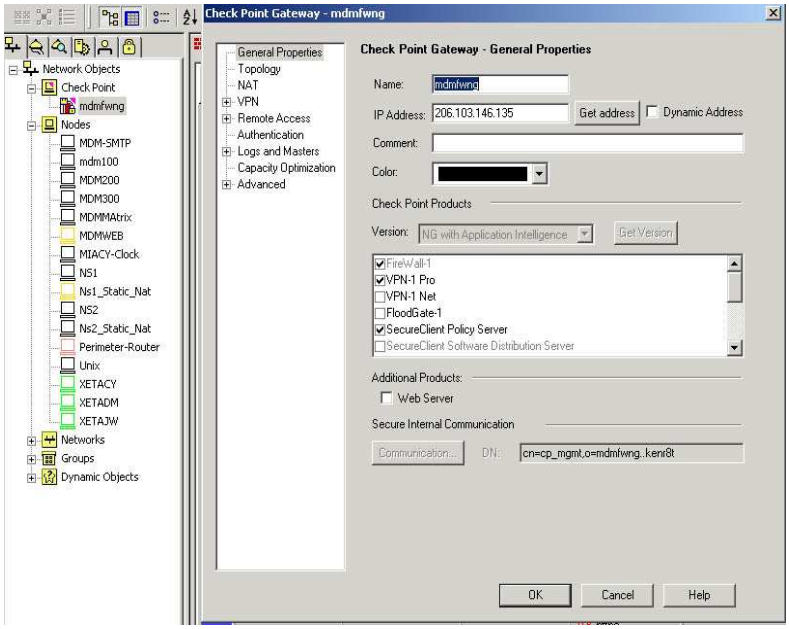


Gráfico 41

Topología de las redes Externa, DMZ e Interna.

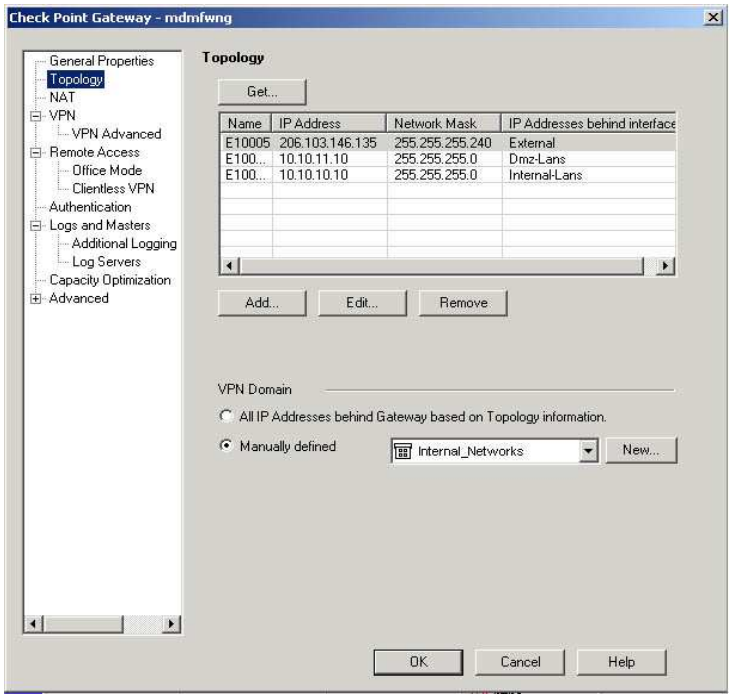


Gráfico 42

Usuarios del Grupo VPN con acceso a LAN interna.

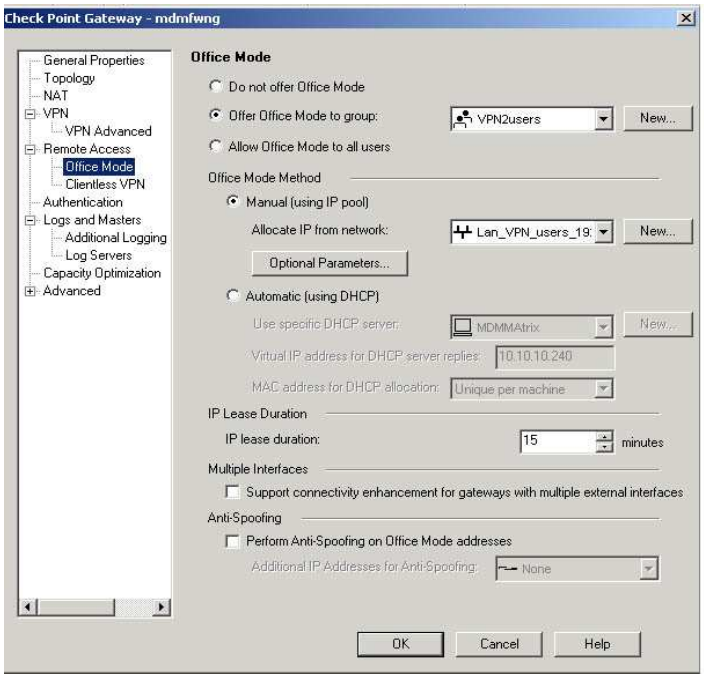


Gráfico 43

Autenticación utilizando usuario y contraseña de Firewall-1.

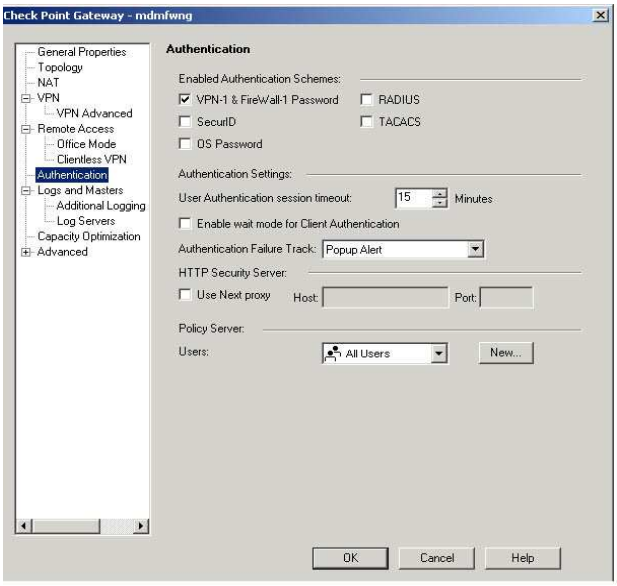


Gráfico 44

Propiedades de los Nodos en el FireWall-1 del Grupo MDM: mdmfwng

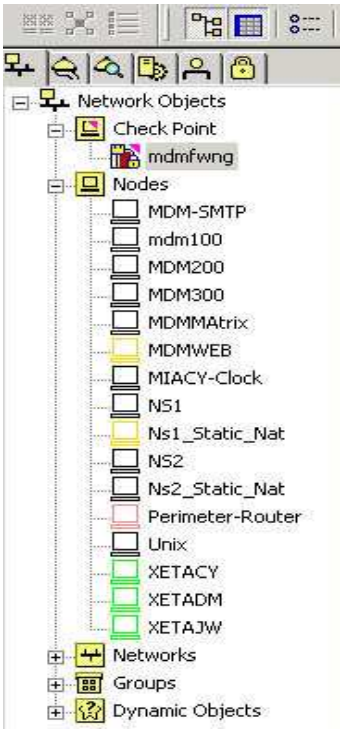


Gráfico 45

El servidor MDM-SMTP es el servidor que utilizan los huéspedes de las tres propiedades para envío de correos electrónicos y se encuentra en la red DMZ 10.10.11.X.

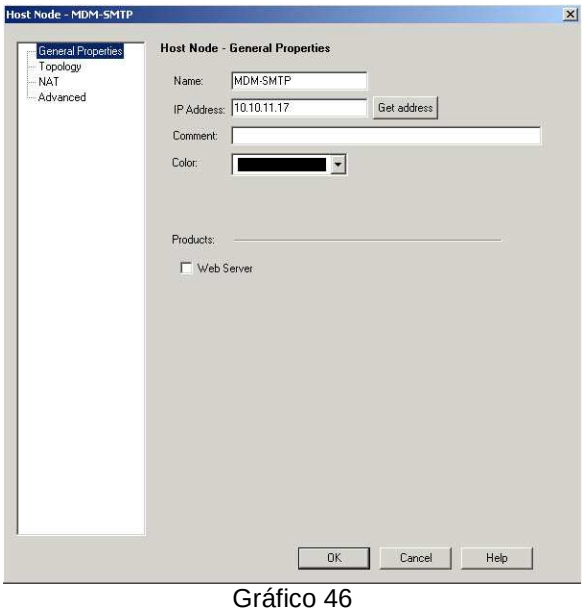


Gráfico 46

La dirección de red 206.103.146.133 la asignada al servidor SMTP por el cual salen los correos de los huéspedes de las tres propiedades.

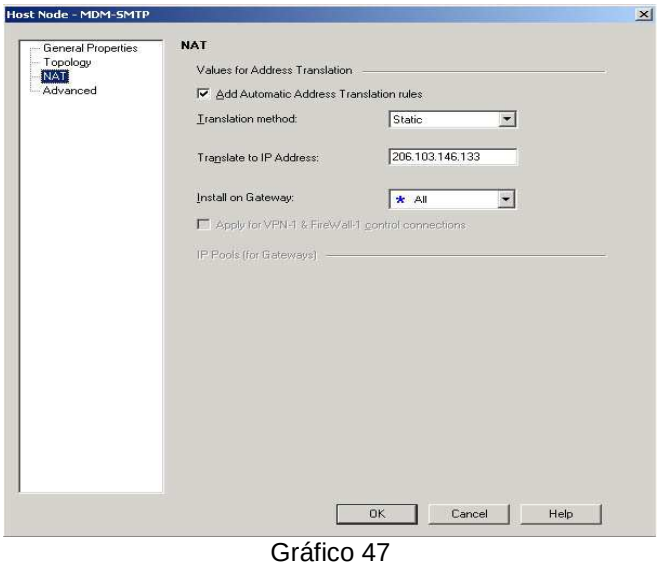


Gráfico 47

El servidor MDM100 es el servidor donde se encuentra instalado Active Directory de la compañía y se encuentra en la red interna 10.10.10.2. Este servidor tiene un uso interno, es uno de los más importantes y su modo de translación NAT se encuentra oculto.

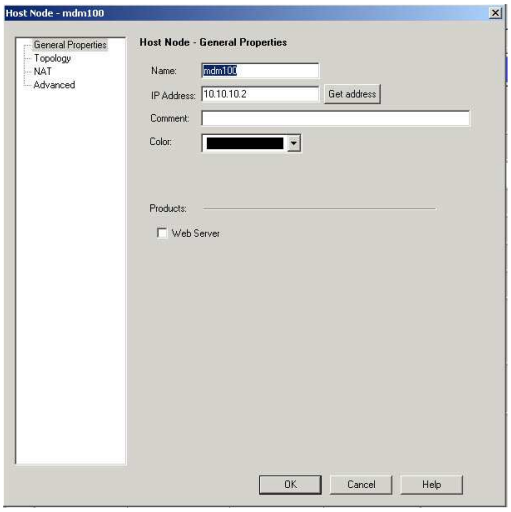


Gráfico 48

En el servidor MDM200 es el servidor de correo electrónico Microsoft Exchange de las propiedades MIADD Y MIACY. Se encuentra en la red 10.10.10.X donde están todos los servidores locales de estas dos propiedades. Realiza un NAT a la dirección 206.103.146.134 por donde salen todos los correos electrónicos de la parte administrativa de MIADD y MIACY

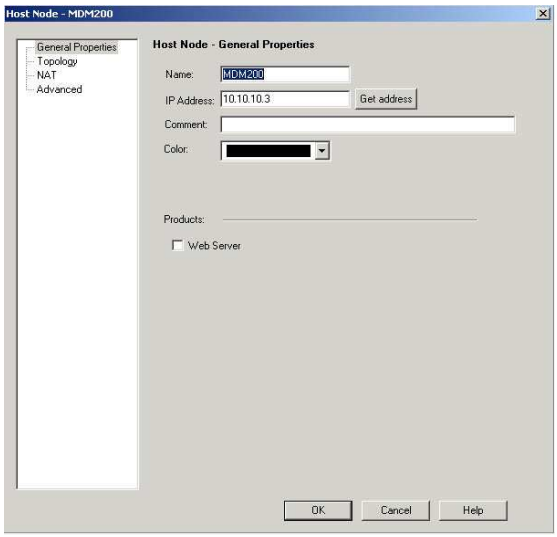


Gráfico 49

En el servidor MDM300 es el servidor de correo electrónico Microsoft Exchange de la propiedad MIAJW. Se encuentra en la red 10.10.30.X donde están todos los servidores locales de esta propiedad. Realiza un NAT a la dirección 206.103.146.139 por donde salen todos los correos electrónicos de la parte administrativa de MIAJW.

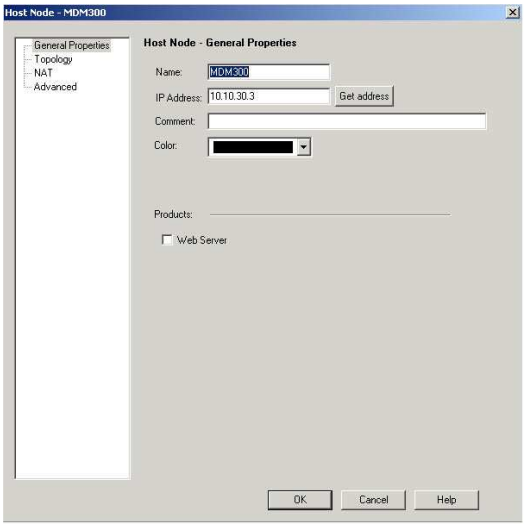
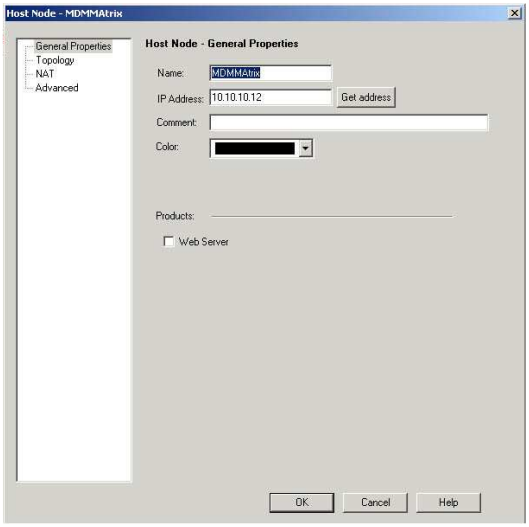


Gráfico 50

En el servidor MDMMatrix se encuentra alojada la aplicación que permite realizar diagramás para los salones de convenciones proporcionado por Marriott. Se encuentra en la red 10.10.10.X que es una red interna, no sale al Internet por lo que no realiza NAT.



Gráfco 51

El servidor MDMWEB, como su nombre lo indica, es el servidor Web del Grupo MDM y se encuentra en la red DMZ 10.10.11.X. Realiza un NAT a la dirección de red externa 206.103.146.132.

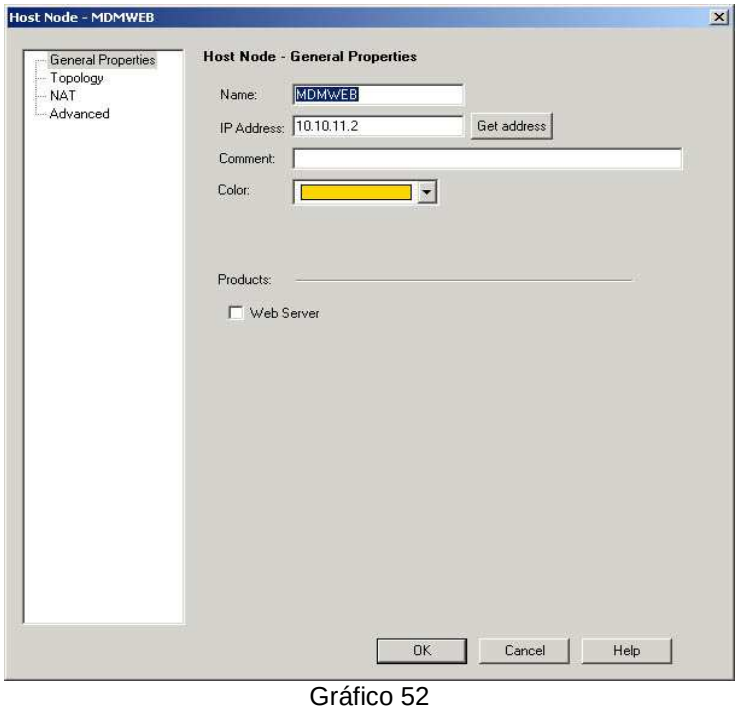


Gráfico 52

Este gráfico muestra la dirección de red del servidor Web.

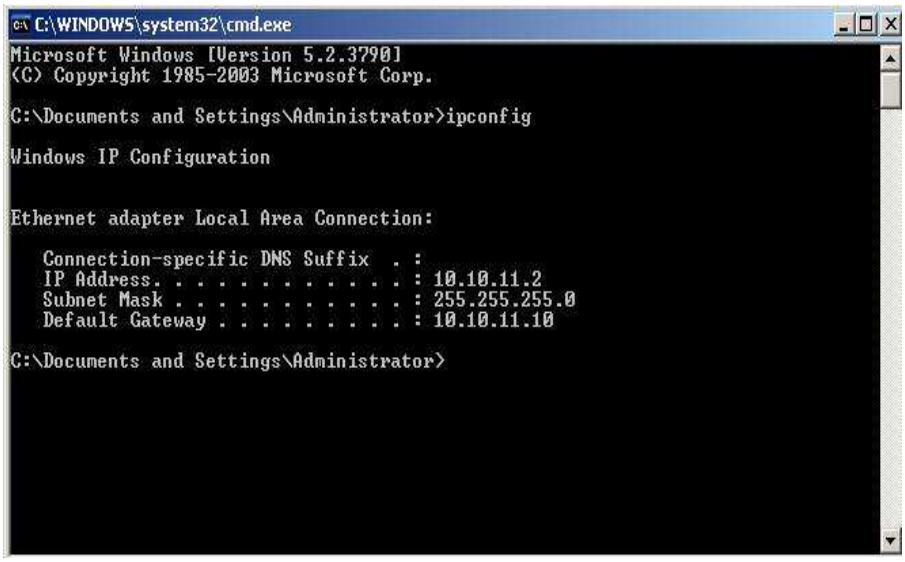


Gráfico 53

El servidor NS1 es el servidor de DNS primario del Grupo MDM y se encuentra en la red DMZ 10.10.11.13. Este servidor es de red local por lo que se debe realizar un NAT para que pueda acceder al Internet. Este NAT se lo hace a la dirección de red 206.103.146.130.

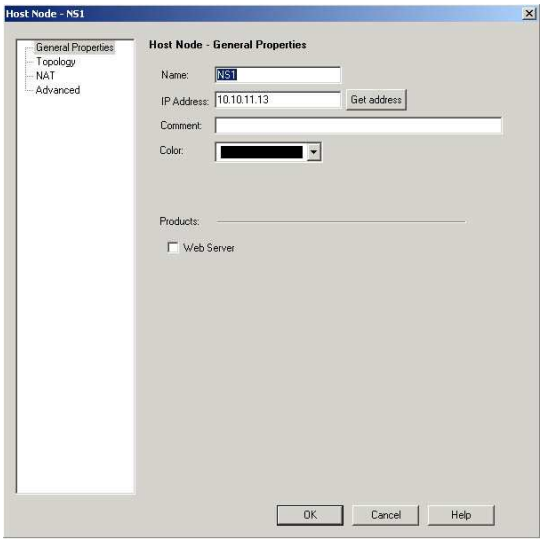


Gráfico 54

El servidor Ns1_Static_Nat es el servidor que posee la dirección estática de red 206.103.146.130 que es la que utiliza el servidor NS1.

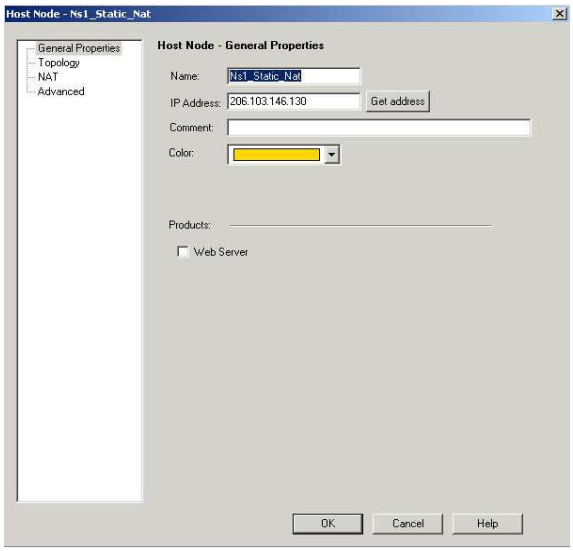


Gráfico 55

El servidor NS2 es el servidor de DNS secundario del Grupo MDM y se encuentra en la red DMZ con dirección de red 10.10.11.11. Realiza un NAT a la direccion de red 206.103.146.131.

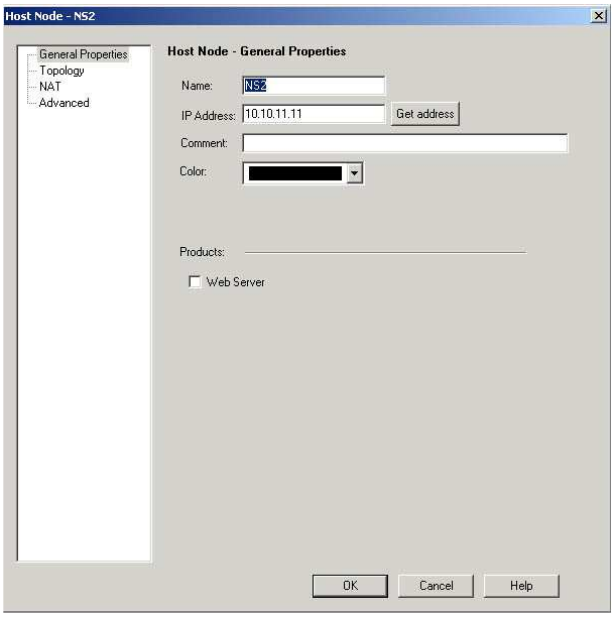


Gráfico 56

El servidor Ns2_Static_Nat es el servidor que posee la dirección estática de red 206.103.146.131 que es la que utiliza el servidor NS2.

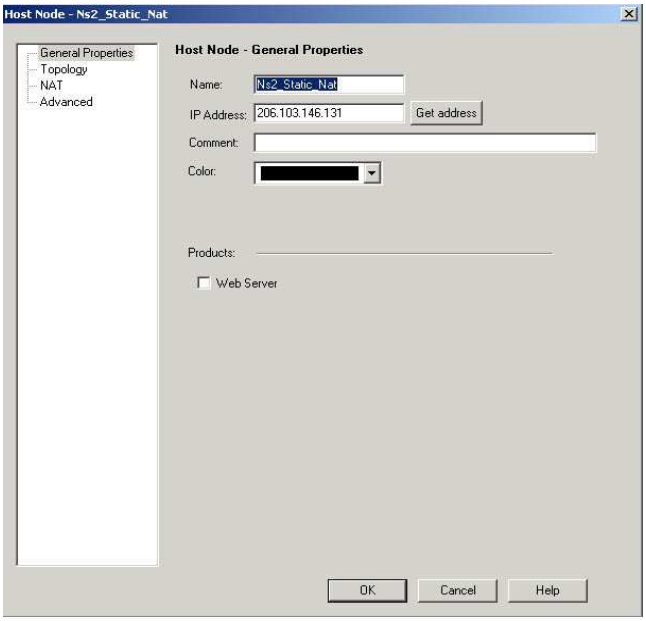


Gráfico 57

El Ruteador Perimetral del Grupo MDM es el que recibe la conexión de Internet. Tiene una dirección de red estática protegida 206.103.146.129.

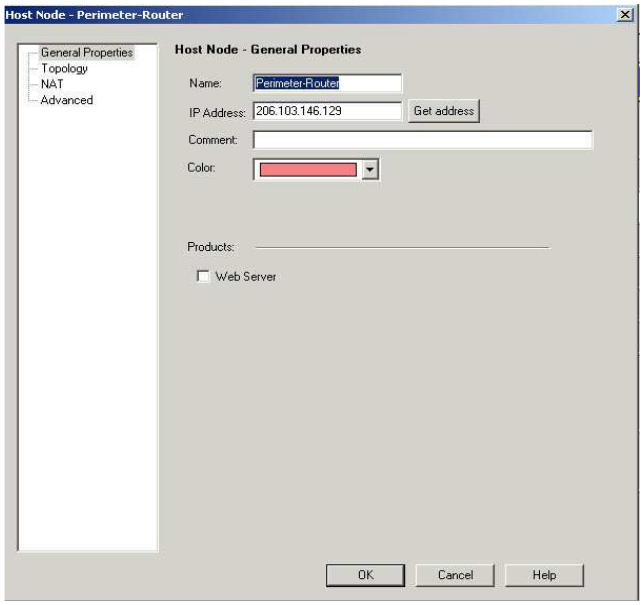


Gráfico 58

El servidor UNIX es el servidor por el cual se realiza la comunicación entre el Grupo MDM y la corporación Marriott. Se encuentra dentro de la red de servidores del Grupo MDM 10.10.10.X. Realiza un NAT a la dirección 206.103.146.138

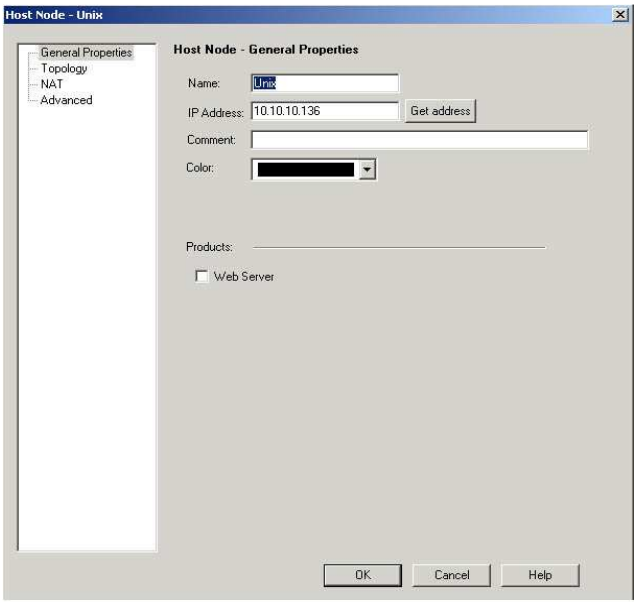


Gráfico 59

El servidor XETACY es la planta telefónica de la propiedad MIACY y se encuentra en la red de servidores internos del Grupo MDM.

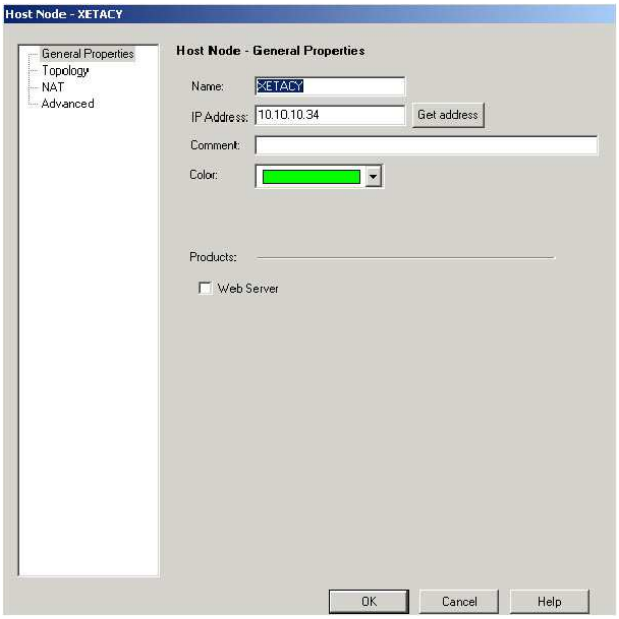


Gráfico 60

El servidor XETADM es la planta telefónica de la propiedad MIADD y se encuentra en la red de servidores internos de esta propiedad. Realiza un NAT a la dirección de red 206.103.146.141.

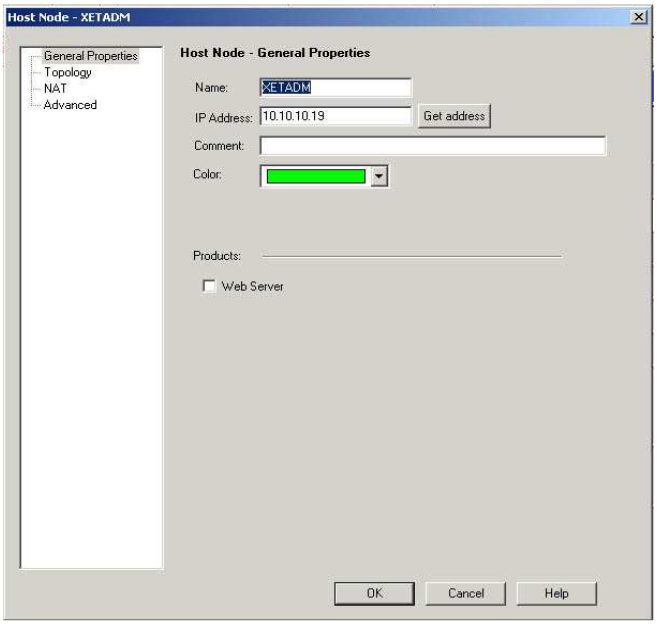


Gráfico 61

Este gráfico demuestra que se accede al servidor XETADM en una máquina de la red 10.10.10.X por medio del Web en la dirección 206.103.146.141.

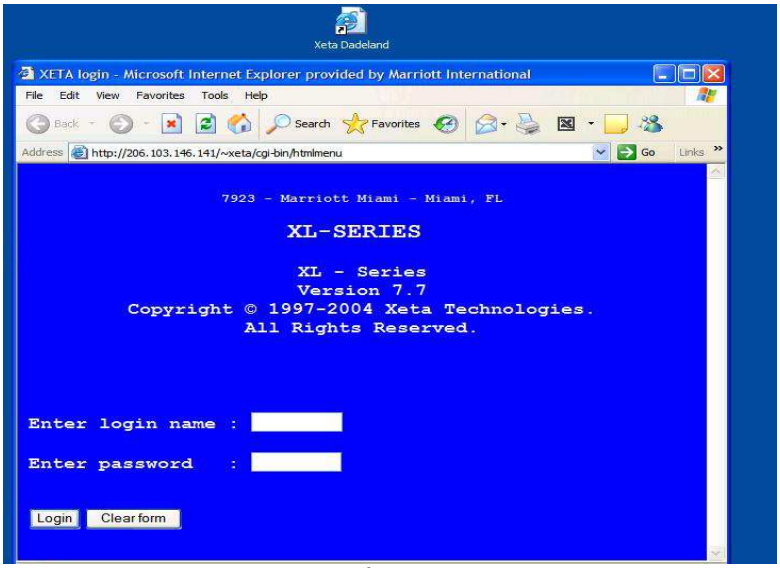


Gráfico 62

El servidor XETAJW es la planta telefónica de la propiedad MIAJW y se encuentra en la red de servidores internos de esta propiedad. Realiza un NAT a la dirección de red 206.103.146.136.

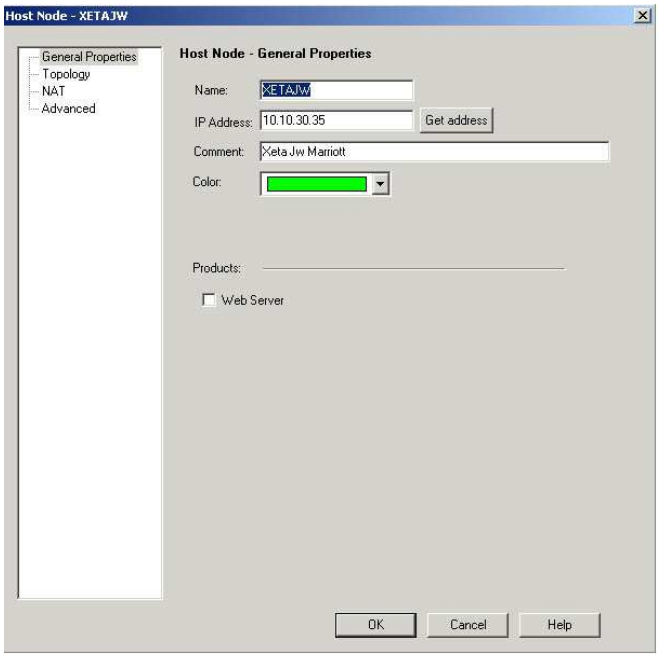


Gráfico 63

Propiedades de los Objetos de Red Redes en el FireWall-1 mdmfwng

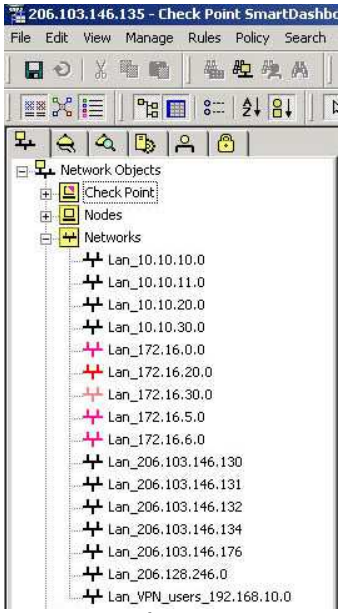


Gráfico 64

Propiedades de la red interna 10.10.10.0. Realiza un NAT bajo la dirección 206.103.146.140.

Gráfico 65

Propiedades de la red DMZ 10.10.11.0. Realiza un NAT bajo la dirección 206.103.146.140.

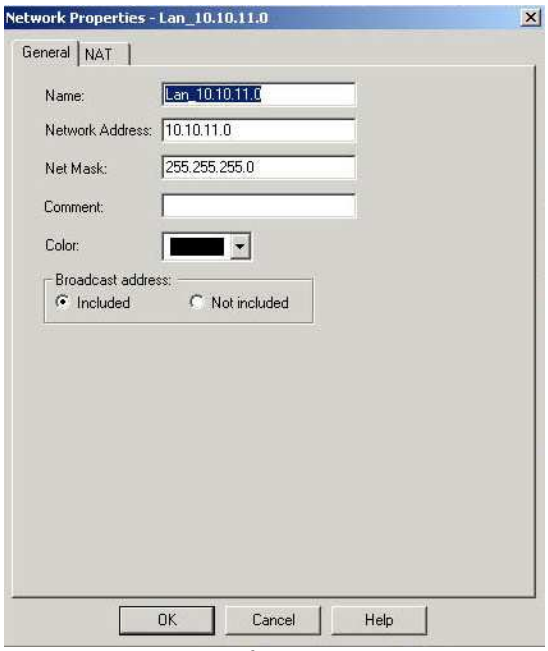


Gráfico 66

Propiedades de la red interna 10.10.10.20. Realiza un NAT bajo la dirección 206.103.146.140.

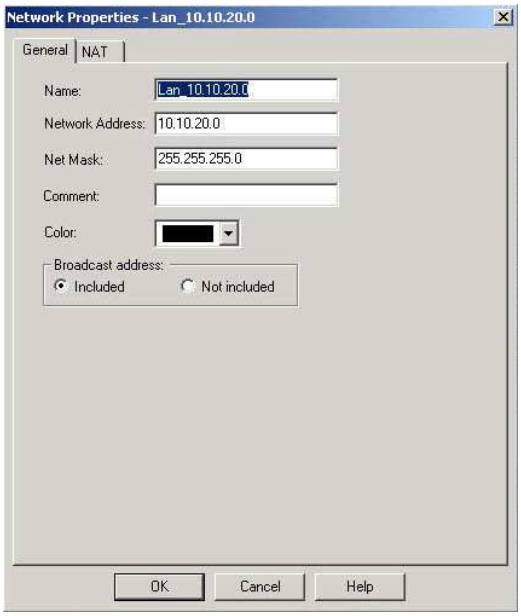


Gráfico 67

Propiedades de la red 10.10.30.0 de la propiedad MIAJW. Realiza un NAT bajo la dirección 206.103.146.140.

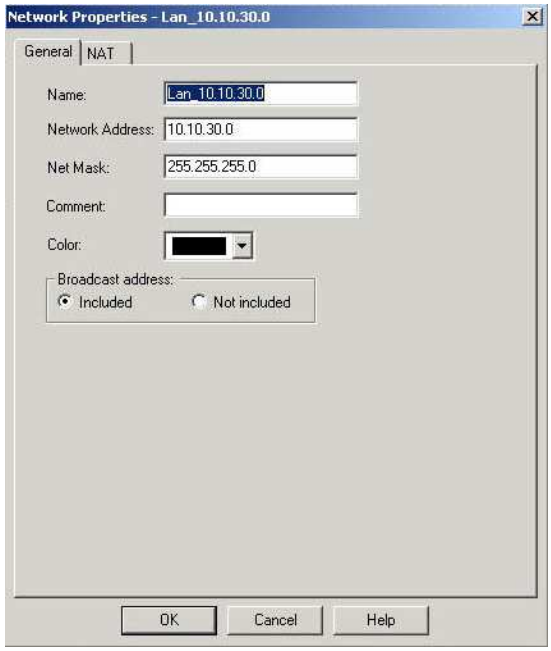


Gráfico 68

Propiedades de la red 172.16.0.0. Realiza un NAT bajo la dirección 206.103.146.140.

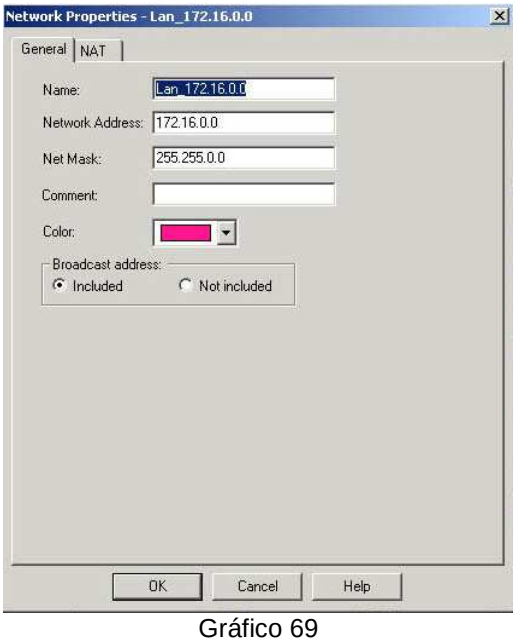


Gráfico 69

Propiedades de la red 172.16.20.0 de Marriott en la propiedad MIADD. Realiza un NAT bajo la dirección 206.103.146.140.

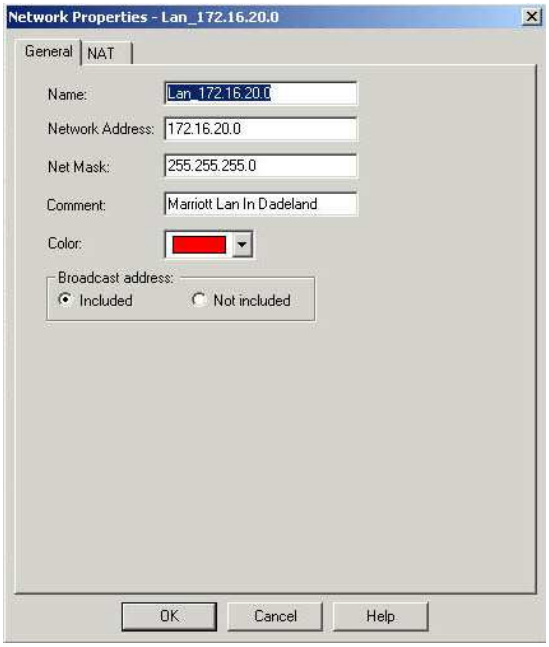


Gráfico 70

Propiedades de la red 172.16.30.0 de Marriott en la propiedad MIAJW. Realiza un NAT bajo la dirección 206.103.146.140.

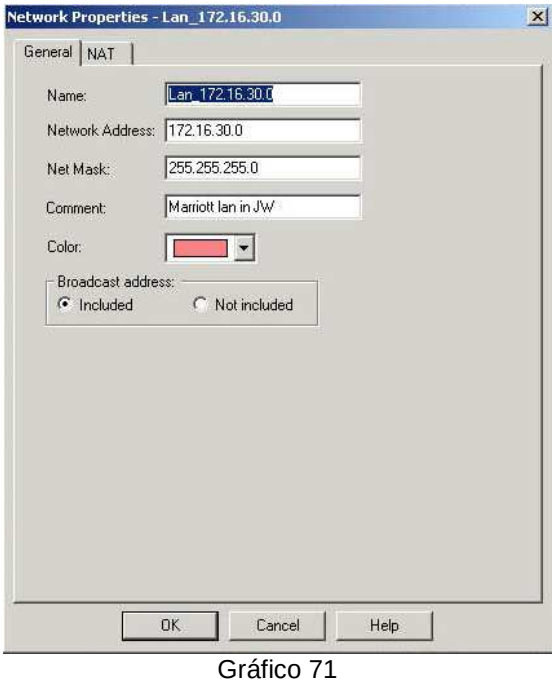


Gráfico 71

Propiedades de la red 172.16.5.0 de Marriott en la propiedad MIAJW. Realiza un NAT bajo la dirección 206.103.146.140.

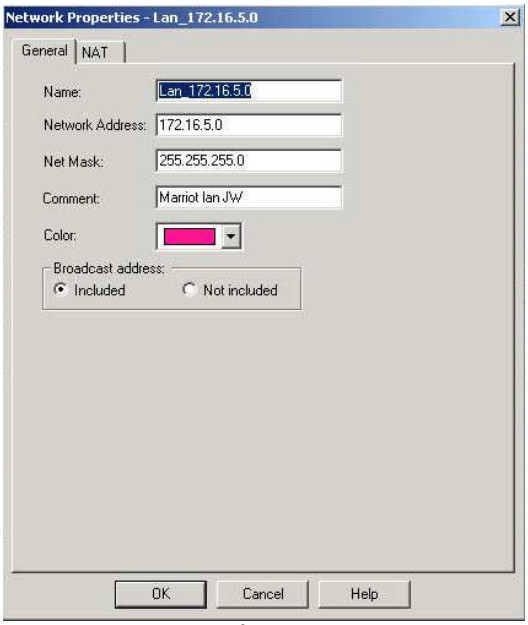


Gráfico 72

Propiedades de la red 172.16.6.0 de Marriott en la propiedad MIADD. Realiza un NAT bajo la dirección 206.103.146.140.

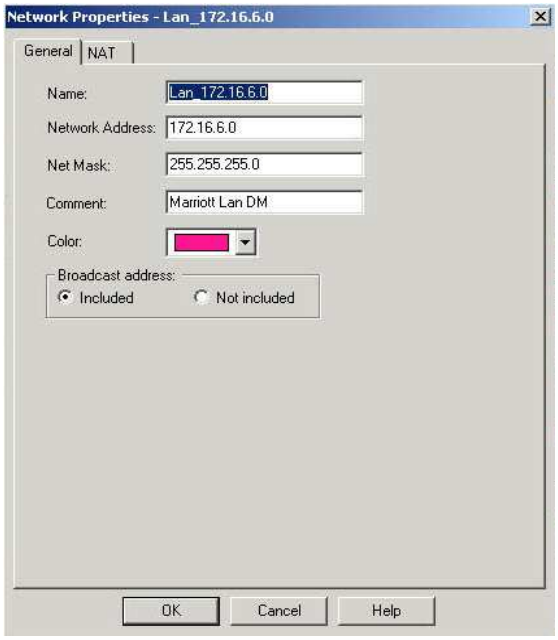


Gráfico 73

Propiedades de la red 206.103.146.130.

Gráfico 74

Propiedades de la red 206.103.146.131.

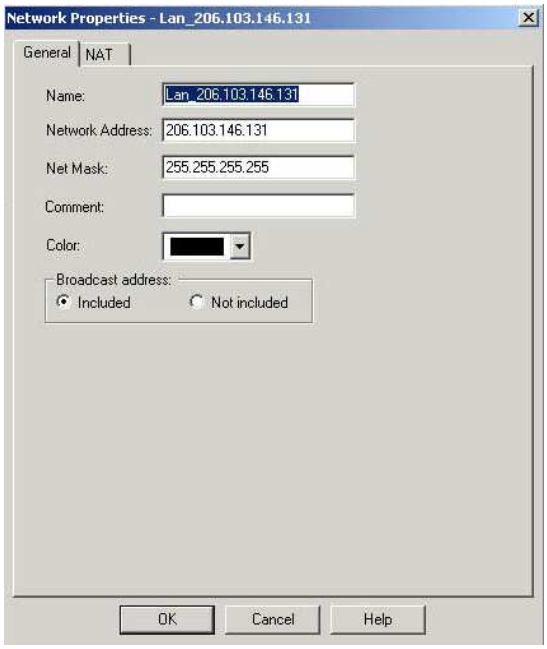


Gráfico 75

Propiedades de la red 206.103.146.132.

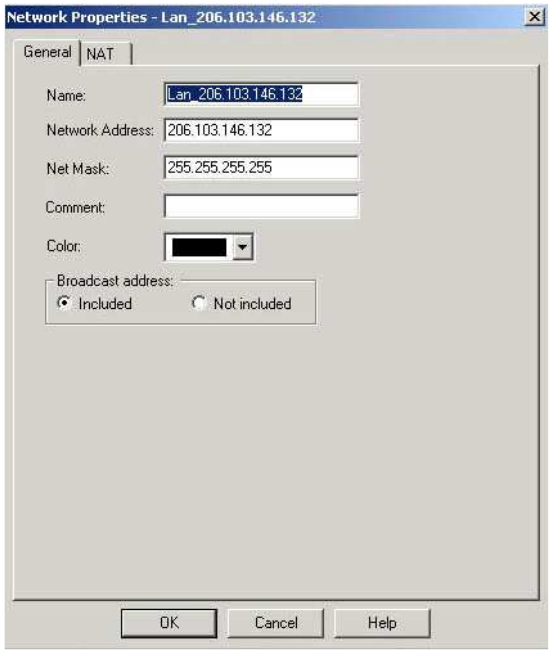


Gráfico 76

Propiedades de la red 206.103.146.134.

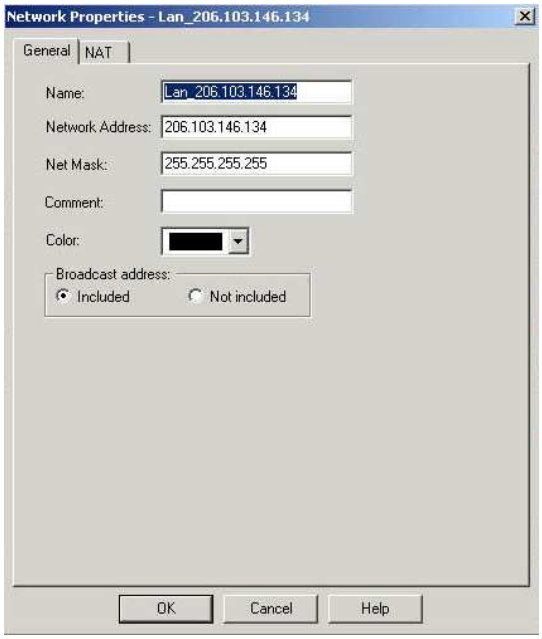


Gráfico 77

Propiedades de la red 206.103.146.176 VPN de la corporación Marriott.

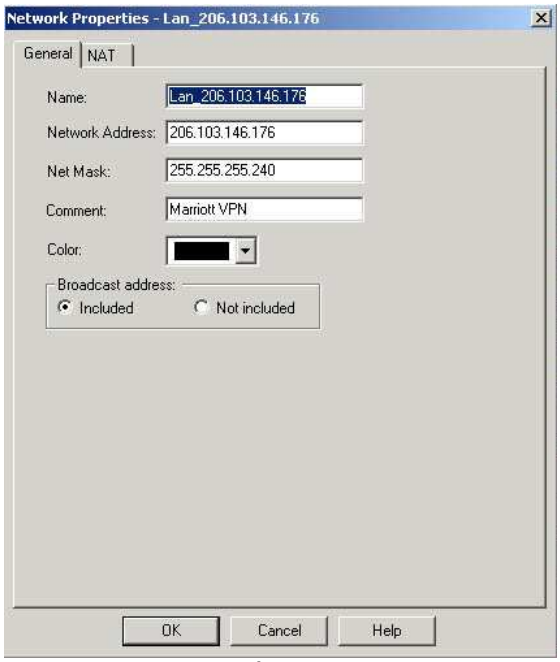


Gráfico 78

Propiedades de la red 206.128.246.0.

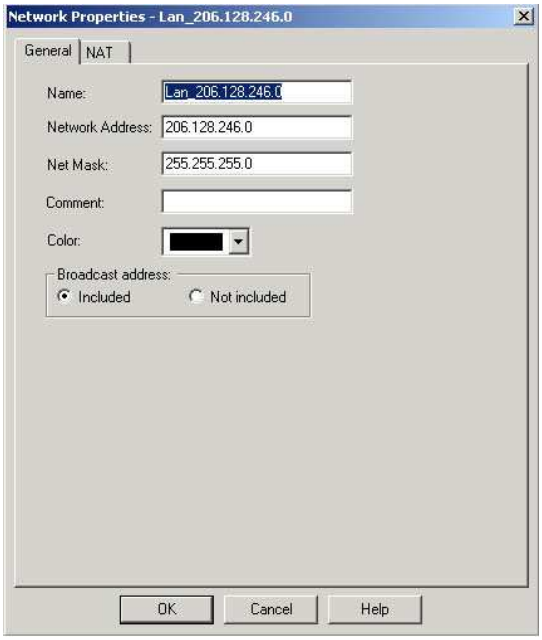


Gráfico 79

Propiedades de la red 192.168.10.0 para los usuarios VPN del Grupo MDM.

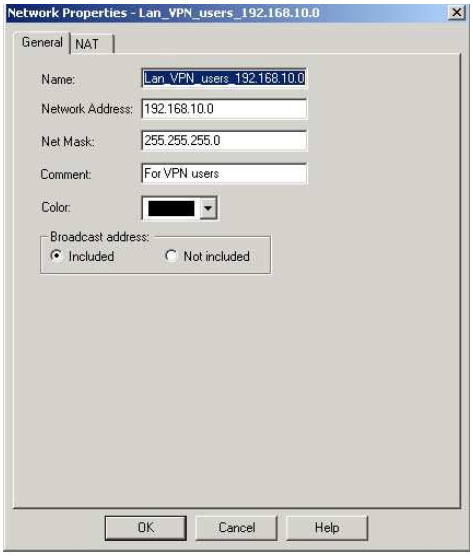


Gráfico 80

Propiedades del Objeto de Red Grupos en el FireWall-1 mdmfwng

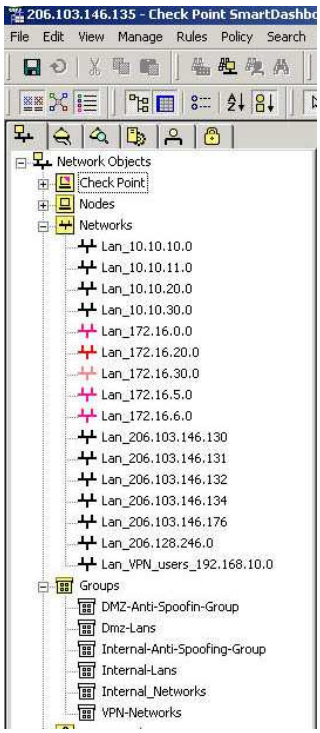


Gráfico 81

Miembros del grupo DMZ Anti-Spoofing.

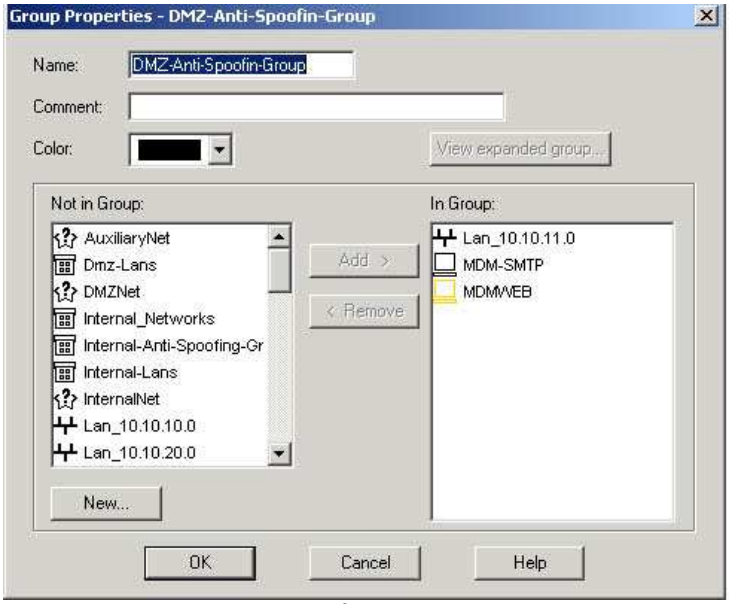


Gráfico 82

Miembros del grupo redes DMZ de área local.

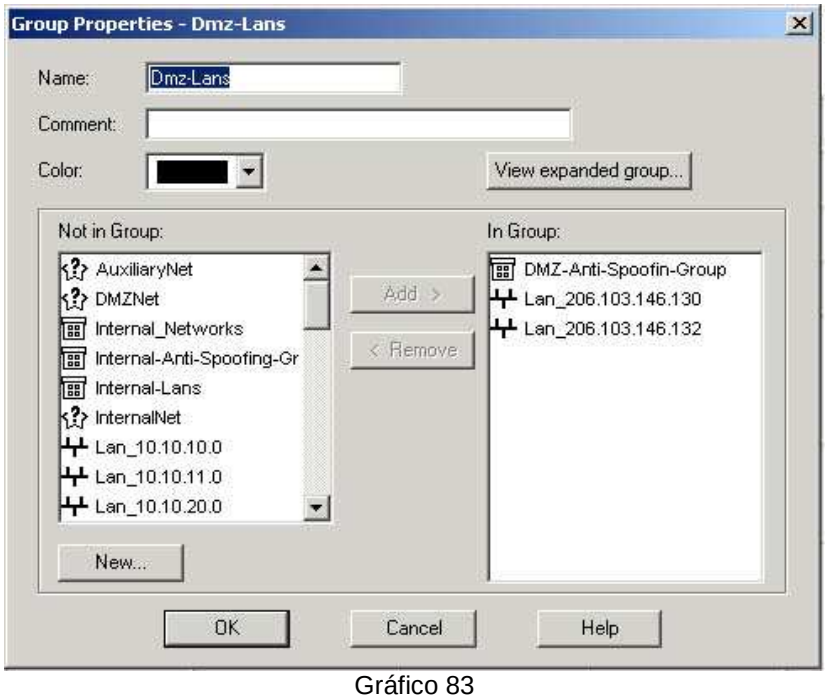


Gráfico 83

Miembros del grupo Anti-Spoofing interno.

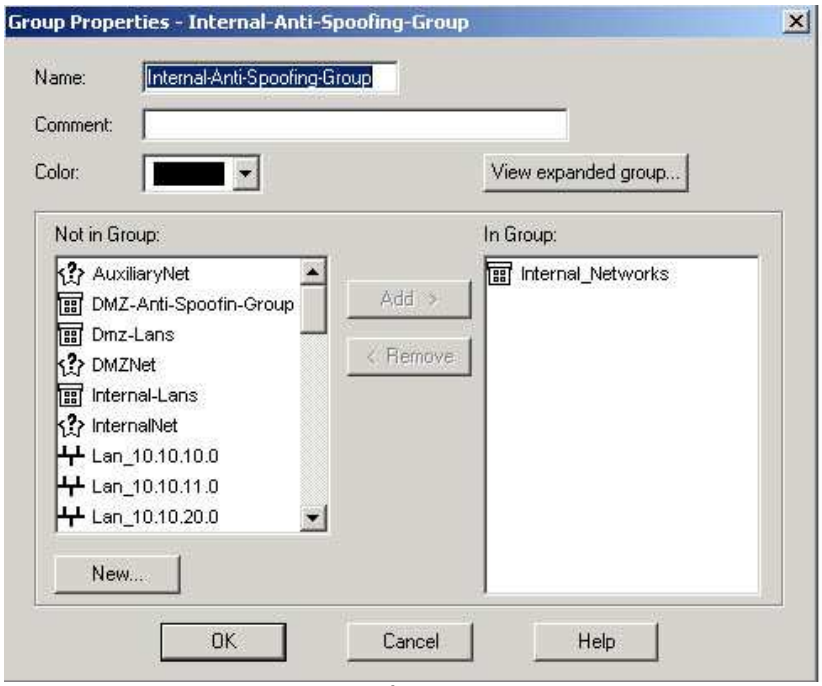


Gráfico 84

Miembros del grupo redes de área local.

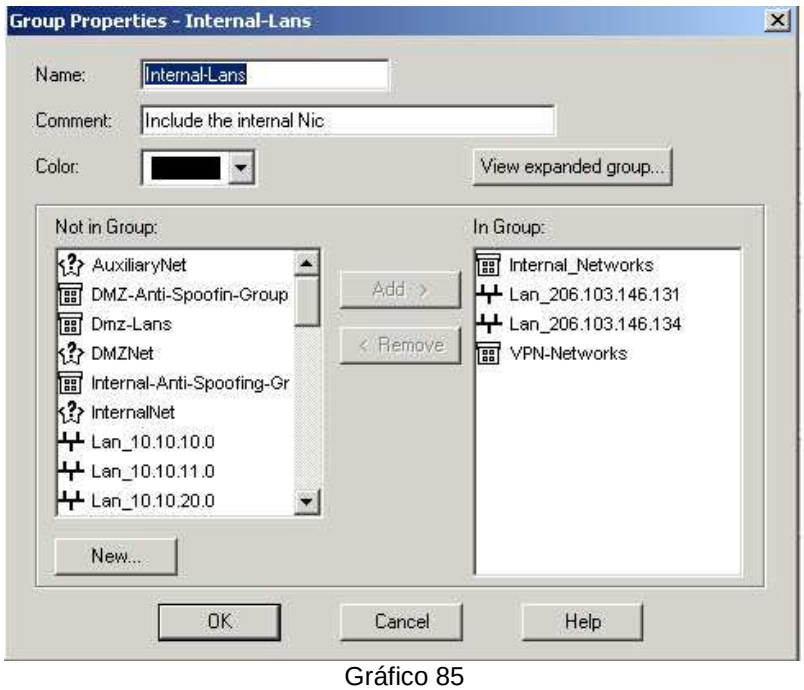


Gráfico 85

Miembros del grupo redes internas.

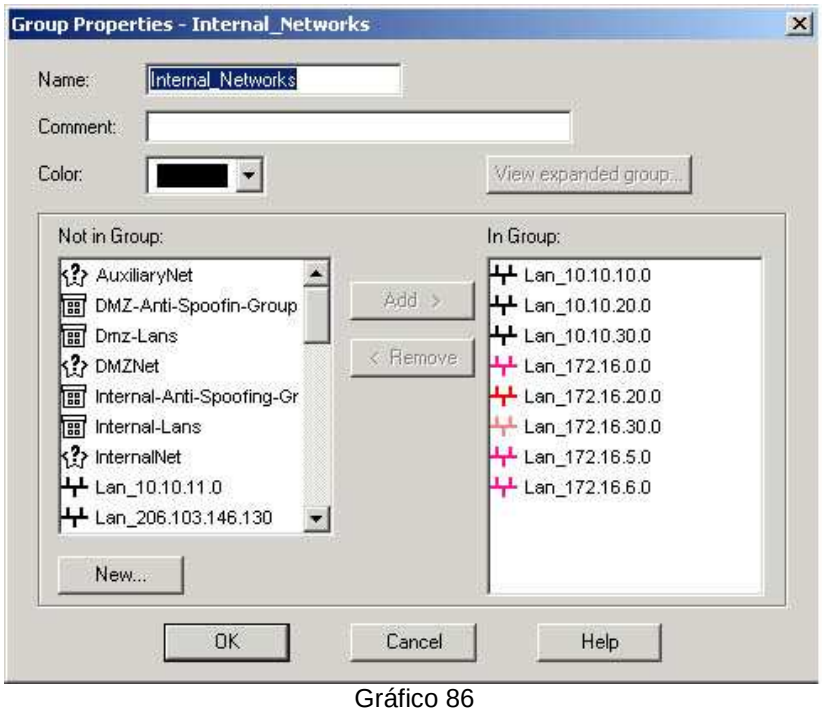


Gráfico 86

Miembros del grupo redes VPN.

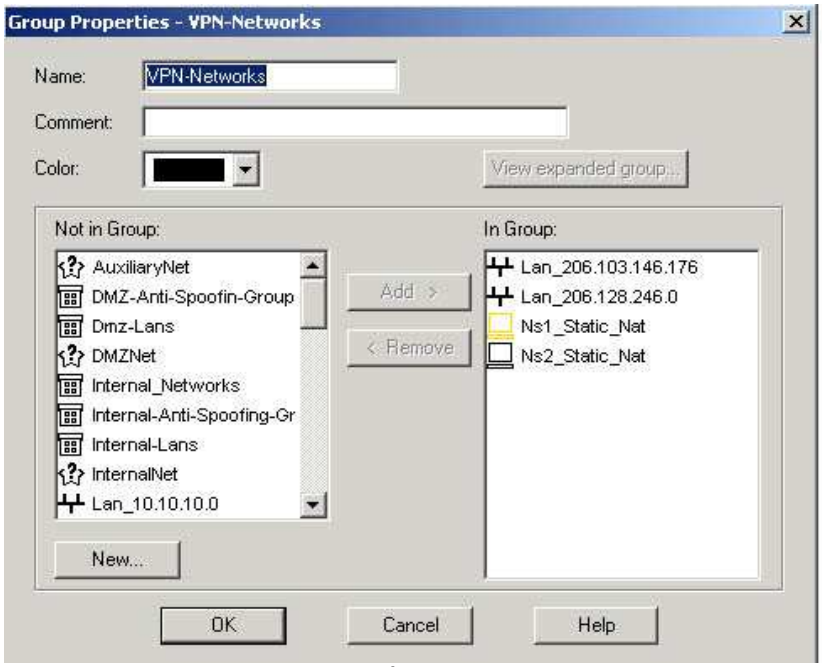


Gráfico 87

Propiedades de los Usuarios VPN en el FireWall-1 mdmfwng.

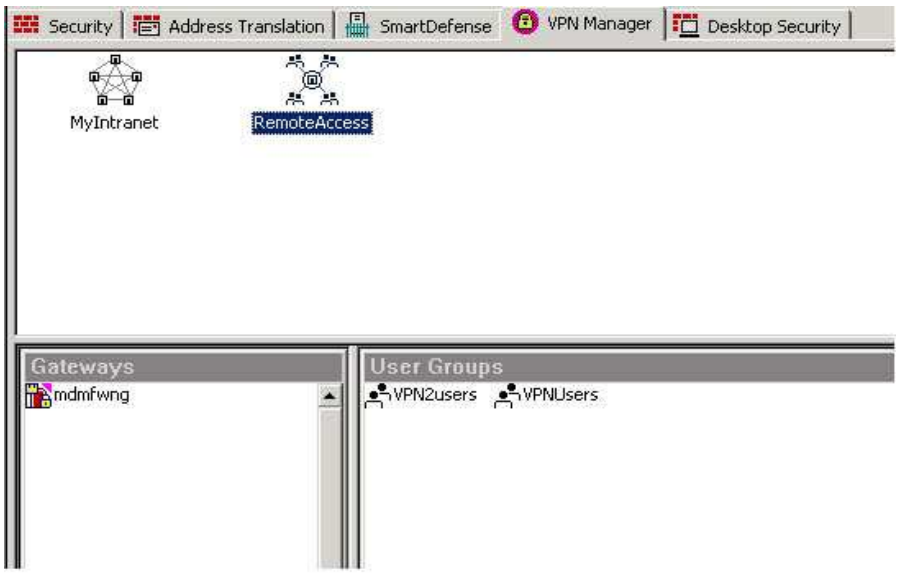


Gráfico 88

Miembros del Grupo VPN VPNUsers.

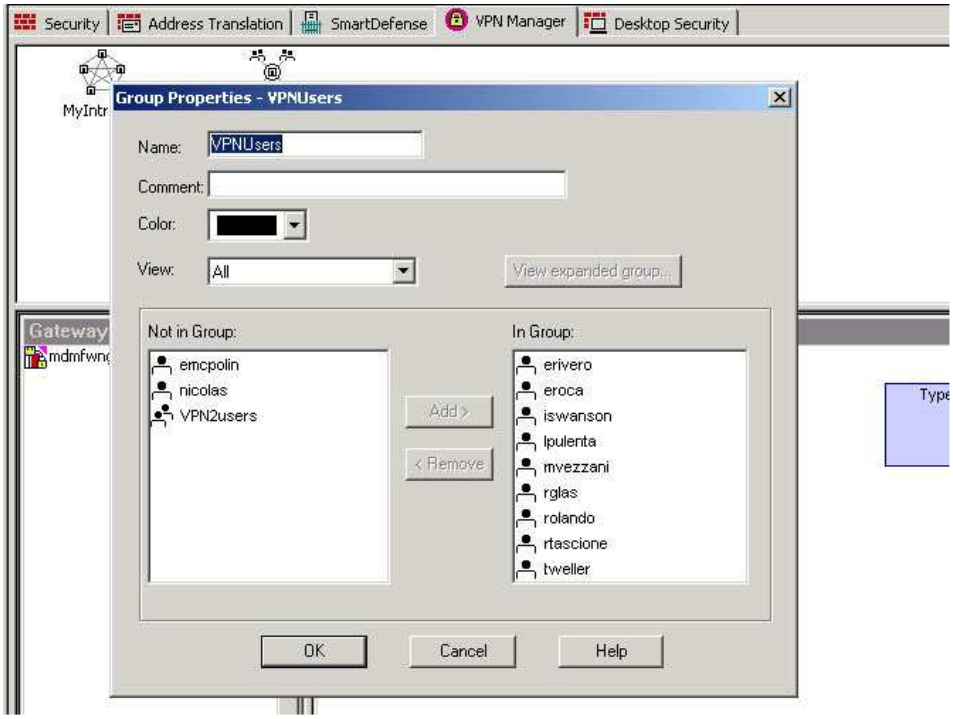


Gráfico 89

Propiedades del usuario rolando (administrador de redes del Grupo MDM). Utiliza contraseña y nombre de usuario de Firewall-1.

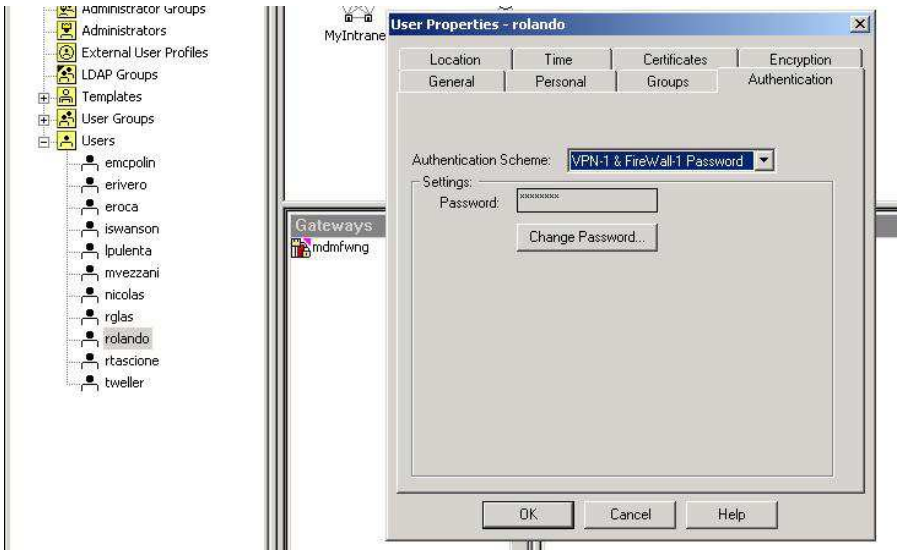


Gráfico 90

Miembro del grupo VPN users.

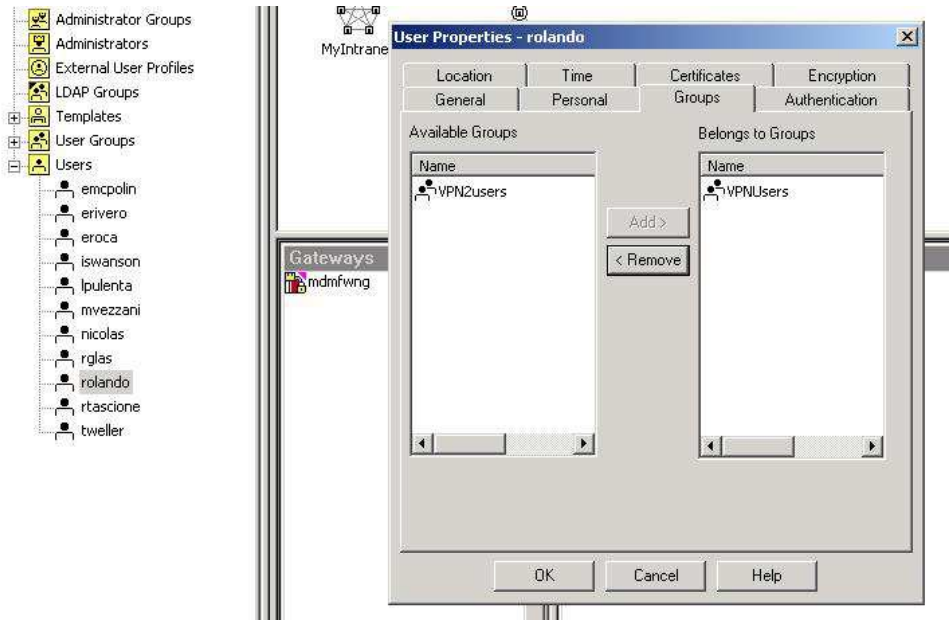


Gráfico 91

El tipo de cifrado utilizado por Firewall-1 es IKE.

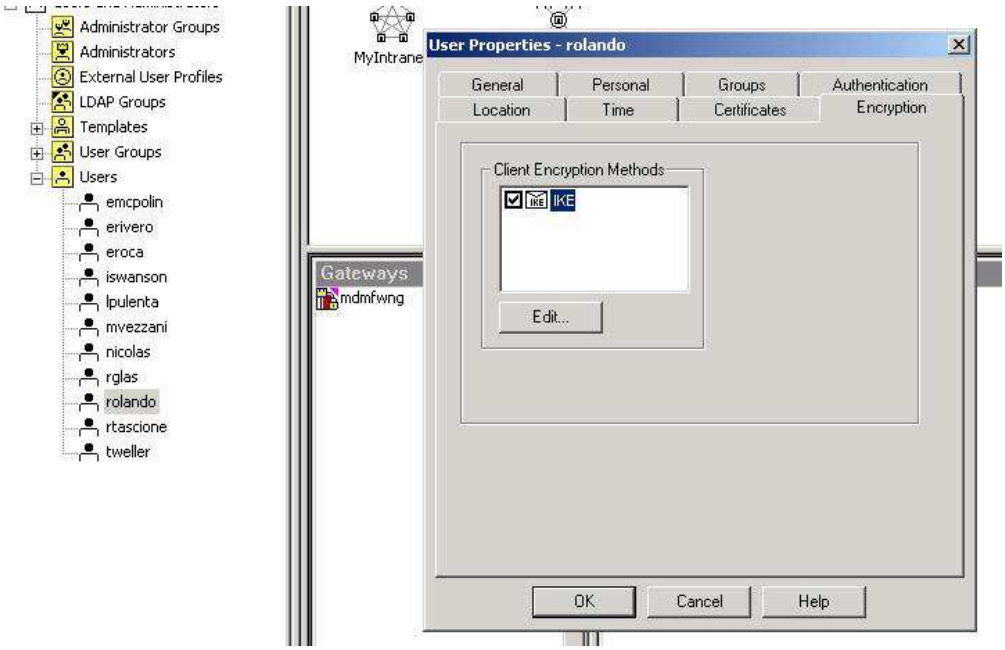


Gráfico 92

Con un algoritmo de cifrado tipo 3DES.

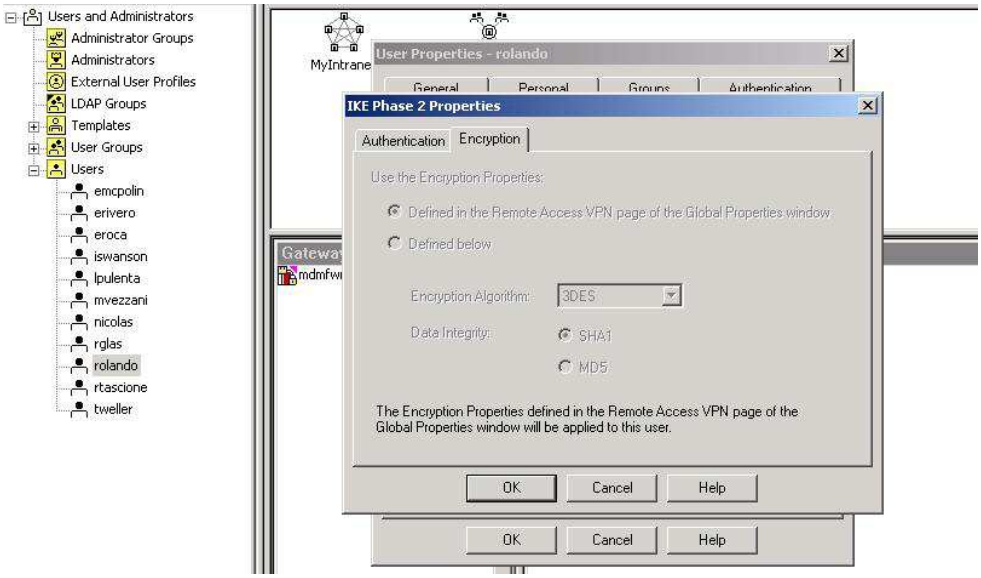


Gráfico 93

La hora y día que este usuario tiene acceso al firewall es ilimitado.

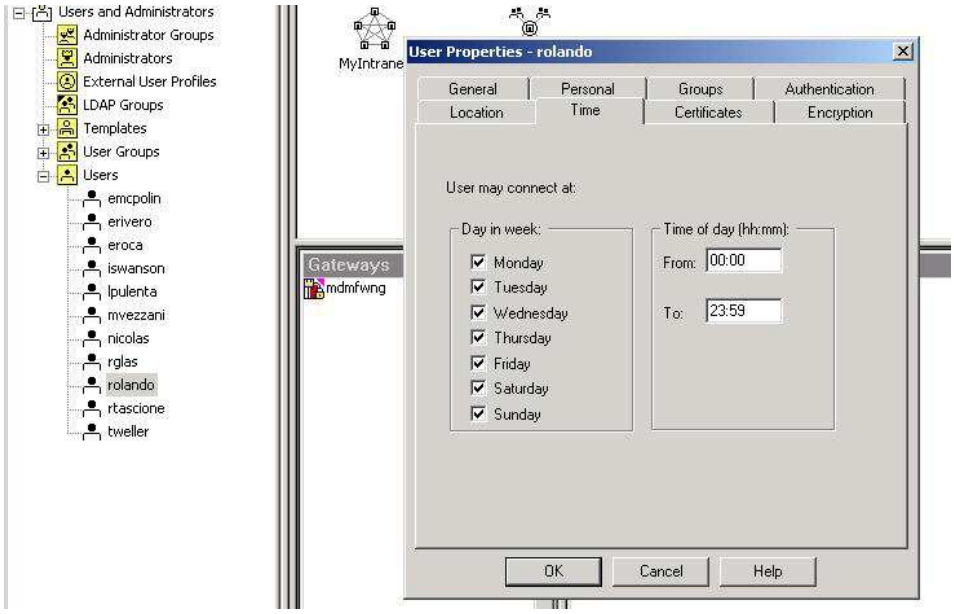


Gráfico 94

Implementación de Políticas de Seguridad utilizadas en el FireWall-1

mdmfwng

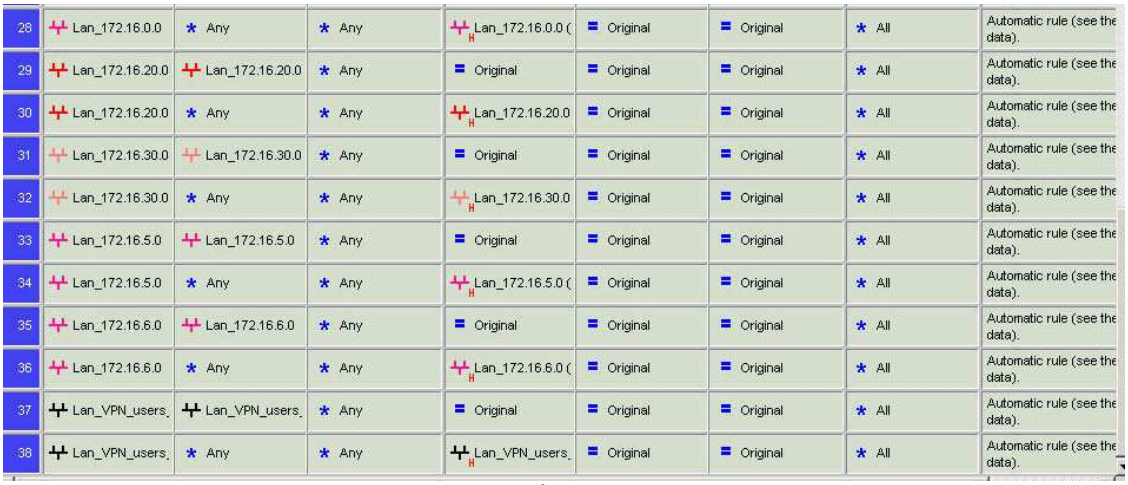
Security | Address Translation | SmartDefense | VPN Manager | Desktop Security

NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME
1	* Any	* Any	* Any Traffic	NBT UDP rip UDP bootp	drop	- None	* Policy Targets	* Any
2	VPN2users@An	* Any	RemoteAccess	* Any	accept	Log	* Policy Targets	* Any
3	Lan_VPN_users_	Lan_10.10.10.0	* Any Traffic	* Any	accept	Log	* Policy Targets	* Any
4	VPNUsers@Any	* Any	RemoteAccess	* Any	accept	Log	* Policy Targets	* Any
5	* Any	mdmfwng	* Any Traffic	FW1_clntauth	accept	Log	* Policy Targets	* Any
6	* Any	NS1 NS2	* Any Traffic	dns TCP http UDP domain-udp FW1_clntauth	accept	Log	* Policy Targets	* Any
7	NS1 NS2	* Any	* Any Traffic	dns TCP http UDP domain-udp	accept	Log	* Policy Targets	* Any
8	* Any	MDM200 MDM300	* Any Traffic	TCP smtp TCP pop-3 TCP http TCP https TCP imap dns	accept	Log	* Policy Targets	* Any
9	MDM200 MDM300	* Any	* Any Traffic	TCP smtp TCP pop-3 TCP http TCP https TCP imap dns	accept	Log	* Policy Targets	* Any
10	* Any	MDMWEB	* Any Traffic	TCP http TCP https	accept	Log	* Policy Targets	* Any
11	* Any	Internal_Networks	* Any Traffic	Trojan_Services TCP DameWare Yahoo_Messeng TCP rtsp	drop	Log	* Policy Targets	* Any
12	* Any	MDM-SMTP	* Any Traffic	TCP smtp	accept	Log	* Policy Targets	* Any
13	MDM-SMTP	* Any	* Any Traffic	TCP smtp	accept	Log	* Policy Targets	* Any
14	VPN-Networks	* Any	* Any Traffic	* Any	accept	Log	* Policy Targets	* Any
	* Any	VPN-Networks	* Any Traffic	Trojan_Services	drop	Log	* Policy Targets	* Any
16	* Any	XETAJW XETADM XETACY	* Any Traffic	TCP http	accept	Log	* Policy Targets	* Any
16	* Any	XETAJW XETADM XETACY	* Any Traffic	TCP http	accept	Log	* Policy Targets	* Any
17	* Any	* Any	* Any Traffic	TCP smtp Yahoo_Messeng TCP rtsp Trojan_Services TCP CrackDown Napster	drop	Log	* Policy Targets	* Any
18	Internal_Network DMZ-Anti-Spoofi	* Any	* Any Traffic	* Any	accept	Log	* Policy Targets	* Any
19	* Any	* Any	* Any Traffic	* Any	drop	- None	* Policy Targets	* Any

Gráfico 95

Funcionamiento de NAT en el FireWall-1 mdmfwng

NO.	ORIGINAL PACKET			TRANSLATED PACKET			INSTALL ON	C
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE		
1	MDM-SMTP	* Any	* Any	MDM-SMTP (Valic	= Original	= Original	* All	Automatic rule (se data).
2	* Any	MDM-SMTP (Valic	* Any	= Original	MDM-SMTP	= Original	* All	Automatic rule (se data).
3	MDM200	* Any	* Any	MDM200 (Valid A	= Original	= Original	* All	Automatic rule (se data).
4	* Any	MDM200 (Valid A	* Any	= Original	MDM200	= Original	* All	Automatic rule (se data).
5	MDM300	* Any	* Any	MDM300 (Valid A	= Original	= Original	* All	Automatic rule (se data).
6	* Any	MDM300 (Valid A	* Any	= Original	MDM300	= Original	* All	Automatic rule (se data).
7	MDMWEB	* Any	* Any	MDMWEB (Valid .	= Original	= Original	* All	Automatic rule (se data).
8	* Any	MDMWEB (Valid .	* Any	= Original	MDMWEB	= Original	* All	Automatic rule (se data).
9	NS1	* Any	* Any	NS1 (Valid Addre	= Original	= Original	* All	Automatic rule (se data).
10	* Any	NS1 (Valid Addre	* Any	= Original	NS1	= Original	* All	Automatic rule (se data).
11	NS2	* Any	* Any	NS2 (Valid Addre	= Original	= Original	* All	Automatic rule (se data).
12	* Any	NS2 (Valid Addre	* Any	= Original	NS2	= Original	* All	Automatic rule (se data).
13	Unix	* Any	* Any	Unix (Valid Addre	= Original	= Original	* All	Automatic rule (se data).
14	* Any	Unix (Valid Addre	* Any	= Original	Unix	= Original	* All	Automatic rule (se data).
15	XETADM	* Any	* Any	XETADM (Valid A	= Original	= Original	* All	Automatic rule (see the data).
16	* Any	XETADM (Valid A	* Any	= Original	XETADM	= Original	* All	Automatic rule (see the data).
17	XETAJW	* Any	* Any	XETAJW (Valid A	= Original	= Original	* All	Automatic rule (see the data).
18	* Any	XETAJW (Valid A	* Any	= Original	XETAJW	= Original	* All	Automatic rule (see the data).
19	Lan_10.10.10.0	Lan_10.10.10.0	* Any	= Original	= Original	= Original	* All	Automatic rule (see the data).
20	Lan_10.10.10.0	* Any	* Any	Lan_10.10.10.0 (	= Original	= Original	* All	Automatic rule (see the data).
21	Lan_10.10.11.0	Lan_10.10.11.0	* Any	= Original	= Original	= Original	* All	Automatic rule (see the data).
22	Lan_10.10.11.0	* Any	* Any	Lan_10.10.11.0 (	= Original	= Original	* All	Automatic rule (see the data).
23	Lan_10.10.20.0	Lan_10.10.20.0	* Any	= Original	= Original	= Original	* All	Automatic rule (see the data).
24	Lan_10.10.20.0	* Any	* Any	Lan_10.10.20.0 (	= Original	= Original	* All	Automatic rule (see the data).
25	Lan_10.10.30.0	Lan_10.10.30.0	* Any	= Original	= Original	= Original	* All	Automatic rule (see the data).
26	Lan_10.10.30.0	* Any	* Any	Lan_10.10.30.0 (	= Original	= Original	* All	Automatic rule (see the data).
27	Lan_172.16.0.0	Lan_172.16.0.0	* Any	= Original	= Original	= Original	* All	Automatic rule (see the data).



28	Lan_172.16.0.0	Any	Any	Lan_172.16.0.0 (	Original	Original	All	Automatic rule (see the data).
29	Lan_172.16.20.0	Lan_172.16.20.0	Any	Original	Original	Original	All	Automatic rule (see the data).
30	Lan_172.16.20.0	Any	Any	Lan_172.16.20.0	Original	Original	All	Automatic rule (see the data).
31	Lan_172.16.30.0	Lan_172.16.30.0	Any	Original	Original	Original	All	Automatic rule (see the data).
32	Lan_172.16.30.0	Any	Any	Lan_172.16.30.0	Original	Original	All	Automatic rule (see the data).
33	Lan_172.16.5.0	Lan_172.16.5.0	Any	Original	Original	Original	All	Automatic rule (see the data).
34	Lan_172.16.5.0	Any	Any	Lan_172.16.5.0 (	Original	Original	All	Automatic rule (see the data).
35	Lan_172.16.6.0	Lan_172.16.6.0	Any	Original	Original	Original	All	Automatic rule (see the data).
36	Lan_172.16.6.0	Any	Any	Lan_172.16.6.0 (	Original	Original	All	Automatic rule (see the data).
37	Lan_VPN_users_	Lan_VPN_users_	Any	Original	Original	Original	All	Automatic rule (see the data).
38	Lan_VPN_users_	Any	Any	Lan_VPN_users_	Original	Original	All	Automatic rule (see the data).

Gráfico 96

6 Conclusiones

6.1 Una vez analizada la teoría y realizado el estudio de las ventajas y propiedades de la aplicación Firewall-1/VPN-1 de Check Point se toma la decisión de utilizarlo en el Grupo MDM.

6.2 Los costos no representan un gran inconveniente a la hora de tomar la decisión de adquirir esta plataforma de Check Point, ya que comparado con el resto de productos del mercado, es aun económicamente más conveniente, sin que esto sea prioridad a la hora de la toma de decisiones, sino, la seguridad de la información del Grupo MDM.

6.3 La aplicación de Check Point cumple con los estándares del mercado para la implementación de seguridades para aplicaciones expuestas al Internet realizando un correcto análisis de los servicios, activación y bloqueo de puertos específicos y resguardar usuarios del Grupo MDM sin importar su ubicación remota, local, punto a punto o inalámbrica.

6.4 La aplicación Firewall-1/VPN-1 permite implementar y hacer cumplir las políticas de seguridad del Grupo MDM de manera eficiente, algo que resulta primordial a la hora de su adquisición.

6.5 El hecho de tener interfaz completamente gráfica y clara permite que la administración del Firewall-1/VPN-1 en el Grupo MDM se convierta en una tarea fácil de realizarla. El poder utilizar una plataforma Windows para su utilización hace que se siga con una línea estándar en cuanto a sistemas operativos de servidores.

6.6 La capacitación de usuarios encargados de administrar y controlar el correcto funcionamiento del firewall resulta más fácilmente realizable, ya que estos trabajan con servidores Windows y administración grafica de las demás aplicaciones.

6.7 Tanto usuarios, servidores, redes y demás equipos que permiten la comunicación dentro del Grupo MDM se encuentran salvaguardados dentro de un ambiente seguro, ajeno de ataques provenientes desde una red insegura como lo es el Internet ya que Firewall-1 bloquea los ataques, aísla maquinas con problemas del resto de la red y enruta paquetes de manera correcta.

6.8 Los usuarios VPN-1 del Grupo MDM pueden conectarse de manera remota desde cualquier parte del mundo, de manera muy sencilla utilizando su nombre de usuario y contraseña, sin darse cuenta que existe una gran robustez en la autenticación y un túnel de seguridad creado por Firewall-1 que es

prácticamente inviolable por personas ajenas a la comunicación.

6.9 El Grupo MDM logra tener independencia de la corporación Marriott en lo que administración de servidores y redes locales se refiere, sin bloquear el acceso a dicha cooperación para que sigan administrando sus equipos de comunicación y lo que es aun más importante, brindando a esta comunicación una seguridad impenetrable por agentes externos.

6.10 Con la arquitectura de Check Point, el tráfico de datos fluye a través de los procesadores y no a través de la CPU central, lo que elimina atascos en el bus de sistema.

6.11 La ejecución del software Check Point NG en la plataforma del Grupo MDM permite a las redes alcanzar altas velocidades, de forma que los usuarios no se ven impedidos por las medidas de seguridad ni limitados a un determinado número de sesiones. Esta arquitectura permite mejorar la productividad por ancho de banda y contribuye a mejorar el aprovechamiento de la compañía.

6.12 El modo de encriptación propio de Check Point, FWZ, lo hace peculiar al no encriptar la cabecera lo que permite que todo paquete llegue a su destino correcto proporcionando tranquilidad a los usuarios.

Luego de realizado el estudio acerca de la implementación de un firewall para el Grupo MDM, se puede recomendar lo siguiente:

- Es indispensable conocer los objetivos de la red. A cuántos usuarios va a estar destinada, qué volumen de tráfico va a tener y la velocidad en tiempos de respuesta que se quiere tener para así decidir la instalación del Firewall correcto.
- Si se tiene un edificio hotelero, lo más recomendable es utilizar el firewall-1/VPN-1 de Check Point, ya que es uno de los eficientes para este tipo de negocio.
- Se recomienda reconocer y estar familiarizado con los tipos de autenticación y encriptación que posea el firewall para que no existan peligros de vulnerabilidad, ni de pérdida, ni de corrupción de la información en conexiones remotas.
- Conocer las plataformas sobre las cuales se va a trabajar ayuda mucho para que no se presenten errores en manejo de las mismas a la hora de instalar un firewall. Si los administradores tienen mayor adaptación a plataformas Unix o Windows, es mejor seguir con la línea que los haga sentir más cómodos. Esto provocara que la administración de la aplicación sea más sencilla.
- Analizar el costo beneficio es muy importante a la hora de tomar una decisión para adquirir un firewall. Se recomienda analizar distintas opciones, sobretodo aquellas que sean más fuertes en el mercado local.

7 Bibliografía

- RATCLIFFE, Andrew*;* SHAH Inti; *Check Point VPN-1/FireWall-1 NG Administration;* Editorial McGraw Hill; 2002.
- WELCH –ALBERNATHY, Daemon*;* SHAH Inti; *Essential Checkpoint Firewall-1: An Installation, Configuration, and Troubleshooting Guide;* Pearson Education Inc.; 2002
- VPN-1/FireWall-1/FlooodGate-1 Application Support Check Point Software Technologies Ltd.
- VPN-1/Secure Client – Secure Remote Access Check Point Software Technologies Ltd.
- www.checkpoint.com
- http://www.checkpoint.com/support/technical/documents/docs_vpn_fw.html
- http://www.textoscientificos.com/redes/firewalls-distribuidos/firewalls/distribuidos/mercado
- http://www.internetworking.ch/display.cfm/id/101001/disp_type/display/filename/101.pdf
- http://www.scc.es/norman/pdfs/NVC_Firewall1_esp.pdf
- https://pricelist.checkpoint.com/pricelist/US/PLUSGeneral/generallist.jsp
- http://www.checkpoint.com/corporate/shareholder_letter/2003/shareholders_letter_2003.pdf

- http://www.checkpoint.com/promoforms/ww/2x/tolly2xww01_ty.html
- http://mrcorp.infosecwriters.com/intro_to_CP.htm
- http://www.checkpoint.com/press/partners/2007/axent0497.html
- http://www.checkpoint.com/support/technical/online_ug/firewall-14.0/vpintro.htm#5307
- http://www.peapod.co.uk/cp_smartcenter.htm
- http://www.wikilearning.com/firewall_1-wkccp-9777-88.htm
- http://www.tks.buffalo.edu/dir_office/mainop/secuRemote/UBREADME.html
- http://comunisfera.blogspot.com/2006/09/definiciones-de-informacin-y-documento.html
- www.segu-info.com.ar/tesis/cap1.pdf
- HUERTA, Antonio Villalón. “Seguridad en Unix y Redes”. Versión 1.2 Digital – Open Publication License v.10.2 de Octubre de 2000. *www.kriptopolis.com*
- http://www.portalx.com.uy/cgi/portalx/Hecon01.EXE?O,0,,0,10310,10301,1039301,2

8 Anexos

Ejemplo 1: Verificación de un intruso en una máquina de la red 10.10.30.X propiedad MIAJW

El Gráfico a continuación muestra como una máquina (PC-JW) de la red 10.10.30.X de la propiedad MIAJW estaba siendo manipulada por un agente externo utilizando de manera sobrecargada el puerto TCP 445 conocido como puerto Microsoft-ds. Este tipo de amenaza ocasiona que la máquina afectada utiliza en un 100% su CPU lo que puede resultar fatal para la misma.
http://www.vnunet.com/vnunet/news/2118428/dos-attack-storms-port-445
Además de este ataque también estaba siendo vulnerada por el servicio epmap que utiliza el puerto TCP 135 y afecta directamente al navegador de Internet haciéndolo que colapse.
http://portland.indymedia.org/en/2004/12/306509.shtml

No.	Date	Time	Orig.	P...	Service	Source	Destination	
7557...	19May2007	11:36:08	mdmf...	tcp	microsoft-ds	PC-JW	10.15.214.127	3
7557...	19May2007	11:36:08	mdmf...	tcp	microsoft-ds	PC-JW	10.10.102.81	3
7557...	19May2007	11:36:08	mdmf...	tcp	epmap	PC-JW	10.10.114.168	3
7557...	19May2007	11:36:08	mdmf...	tcp	microsoft-ds	PC-JW	10.10.150.113	3
7557...	19May2007	11:36:08	mdmf...	tcp	microsoft-ds	PC-JW	10.10.146.17	3
7557...	19May2007	11:36:08	mdmf...	tcp	epmap	PC-JW	10.10.183.133	3
7557...	19May2007	11:36:08	mdmf...	tcp	epmap	PC-JW	10.15.214.151	3
7557...	19May2007	11:36:08	mdmf...	tcp	epmap	PC-JW	10.10.85.79	3
7557...	19May2007	11:36:08	mdmf...	tcp	epmap	PC-JW	10.10.247.148	3
7557...	19May2007	11:36:08	mdmf...	tcp	microsoft-ds	PC-JW	10.10.220.200	3
7557...	19May2007	11:36:08	mdmf...	tcp	epmap	PC-JW	10.15.214.152	3
7557...	19May2007	11:36:08	mdmf...	tcp	epmap	PC-JW	10.15.214.153	3
7557...	19May2007	11:36:08	mdmf...	tcp	microsoft-ds	PC-JW	10.15.214.129	3
7557...	19May2007	11:36:08	mdmf...	tcp	microsoft-ds	PC-JW	10.15.214.128	3
7557...	19May2007	11:36:08	mdmf...	tcp	smtp	89.0.127.173	206.103.146.134	10
7557...	19May2007	11:36:08	mdmf...	tcp	microsoft-ds	PC-JW	10.10.134.58	3
7557...	19May2007	11:36:08	mdmf...	tcp	epmap	PC-JW	10.10.34.219	3
7557...	19May2007	11:36:08	mdmf...	tcp	https	206.103.146.140	bkvtrack.com	
7557...	19May2007	11:36:08	mdmf...	tcp	epmap	PC-JW	10.10.194.213	3
7557...	19May2007	11:36:08	mdmf...	tcp	microsoft-ds	PC-JW	10.15.214.130	3
7557...	19May2007	11:36:08	mdmf...	tcp	microsoft-ds	PC-JW	10.10.127.35	3
7557...	19May2007	11:36:09	mdmf...	tcp	27186	222.91.124.70	206.128.246.22	
7557...	19May2007	11:36:09	mdmf...	tcp	microsoft-ds	PC-JW	10.10.221.106	3
7557...	19May2007	11:36:09	mdmf...	tcp	microsoft-ds	PC-JW	10.10.101.79	3
7557...	19May2007	11:36:09	mdmf...	tcp	microsoft-ds	PC-JW	10.10.224.124	3
7557...	19May2007	11:36:09	mdmf...	tcp	microsoft-ds	PC-JW	10.10.92.150	3
7557...	19May2007	11:36:09	mdmf...	tcp	microsoft-ds	PC-JW	10.10.148.62	3
7557...	19May2007	11:36:09	mdmf...	tcp	microsoft-ds	PC-JW	10.10.21.192	3
7557...	19May2007	11:36:09	mdmf...	tcp	microsoft-ds	PC-JW	10.10.91.230	3
7557...	19May2007	11:36:09	mdmf...	tcp	epmap	PC-JW	10.10.26.73	3
7557...	19May2007	11:36:09	mdmf...	tcp	microsoft-ds	PC-JW	10.10.54.12	3

Gráfico 97

Cuando se detectó el ataque se procedió a bloquear todo tipo de tráfico desde y hacia la máquina (PC-JW) hasta poder determinar cuál era la causa de este ataque.

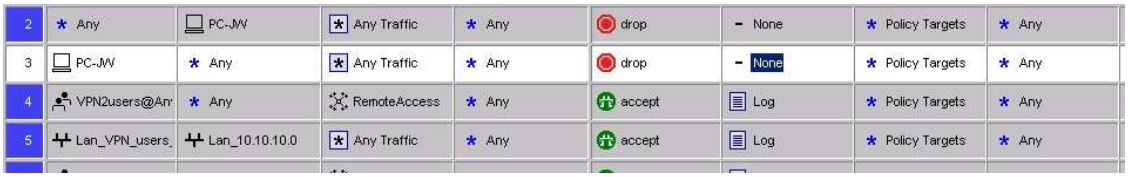


Gráfico 98

Una vez confirmado que esta máquina era la afectada se aplicó la respectiva regla y se aplicó de tal manera que no guarde ningún registro para no tener mensajes repetitivos de algo que ya se conocía estaba ocurriendo.

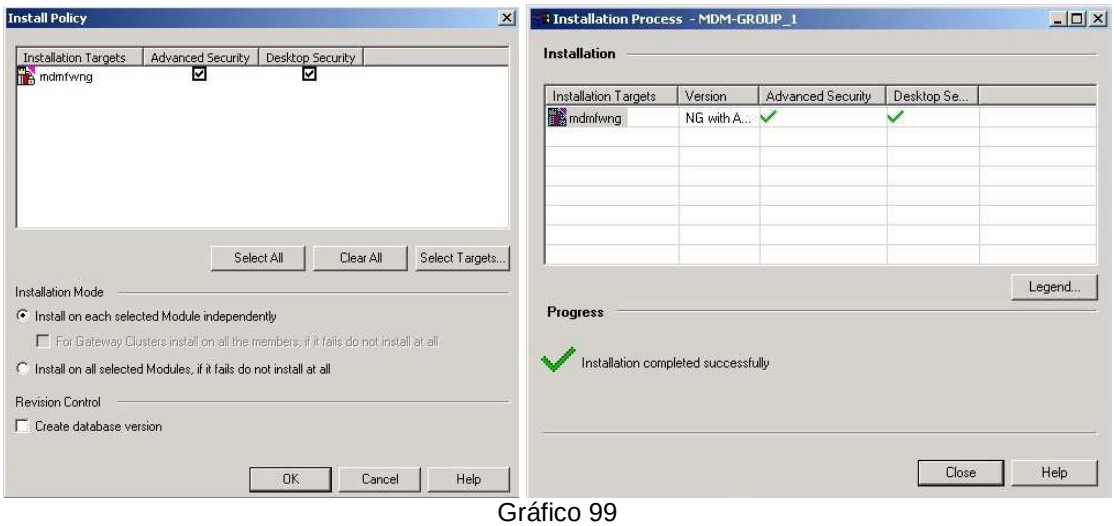
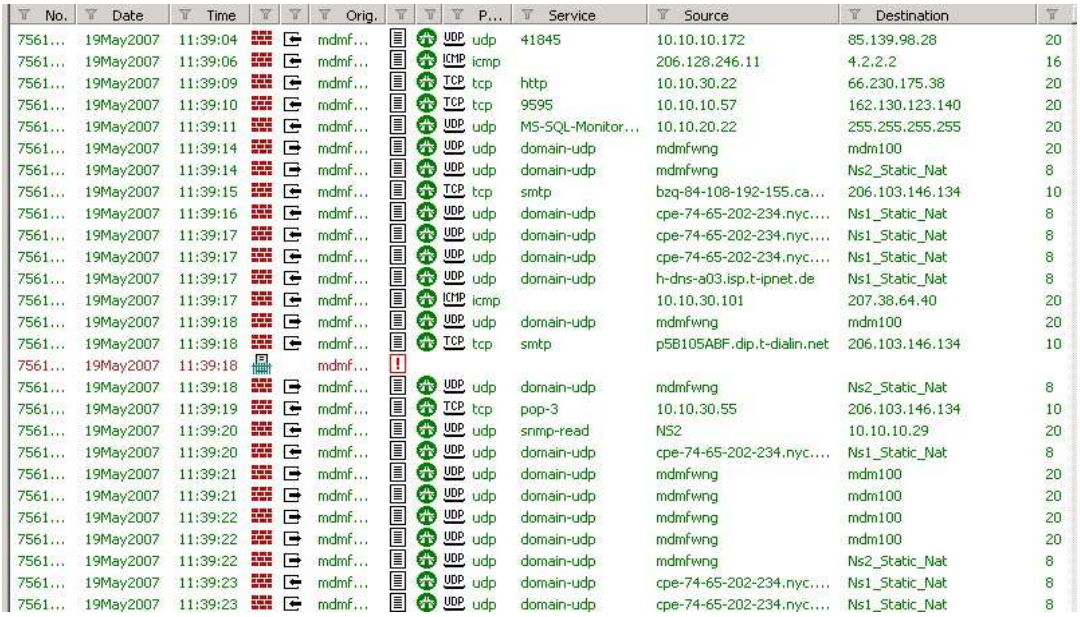


Gráfico 99



No.	Date	Time	Orig.	P...	Service	Source	Destination	
7561...	19May2007	11:39:04	mdmf...	udp	41845	10.10.10.172	85.139.98.28	20
7561...	19May2007	11:39:06	mdmf...	icmp		206.128.246.11	4.2.2.2	16
7561...	19May2007	11:39:09	mdmf...	tcp	http	10.10.30.22	66.230.175.38	20
7561...	19May2007	11:39:10	mdmf...	tcp	9595	10.10.10.57	162.130.123.140	20
7561...	19May2007	11:39:11	mdmf...	udp	MS-SQL-Monitor...	10.10.20.22	255.255.255.255	20
7561...	19May2007	11:39:14	mdmf...	udp	domain-udp	mdmfwng	mdm100	20
7561...	19May2007	11:39:14	mdmf...	udp	domain-udp	mdmfwng	Ns2_Static_Nat	8
7561...	19May2007	11:39:15	mdmf...	tcp	smtp	bzq-84-108-192-155.ca...	206.103.146.134	10
7561...	19May2007	11:39:16	mdmf...	udp	domain-udp	cpe-74-65-202-234.nyc....	Ns1_Static_Nat	8
7561...	19May2007	11:39:17	mdmf...	udp	domain-udp	cpe-74-65-202-234.nyc....	Ns1_Static_Nat	8
7561...	19May2007	11:39:17	mdmf...	udp	domain-udp	cpe-74-65-202-234.nyc....	Ns1_Static_Nat	8
7561...	19May2007	11:39:17	mdmf...	udp	domain-udp	h-dns-a03.isp.t-ipnet.de	Ns1_Static_Nat	8
7561...	19May2007	11:39:17	mdmf...	icmp		10.10.30.101	207.38.64.40	20
7561...	19May2007	11:39:18	mdmf...	udp	domain-udp	mdmfwng	mdm100	20
7561...	19May2007	11:39:18	mdmf...	tcp	smtp	p5B105ABF.dip.t-dialin.net	206.103.146.134	10
7561...	19May2007	11:39:18	mdmf...					
7561...	19May2007	11:39:18	mdmf...	udp	domain-udp	mdmfwng	Ns2_Static_Nat	8
7561...	19May2007	11:39:19	mdmf...	tcp	pop-3	10.10.30.55	206.103.146.134	10
7561...	19May2007	11:39:20	mdmf...	udp	snmp-read	NS2	10.10.10.29	20
7561...	19May2007	11:39:20	mdmf...	udp	domain-udp	cpe-74-65-202-234.nyc....	Ns1_Static_Nat	8
7561...	19May2007	11:39:21	mdmf...	udp	domain-udp	mdmfwng	mdm100	20
7561...	19May2007	11:39:21	mdmf...	udp	domain-udp	mdmfwng	mdm100	20
7561...	19May2007	11:39:22	mdmf...	udp	domain-udp	mdmfwng	mdm100	20
7561...	19May2007	11:39:22	mdmf...	udp	domain-udp	mdmfwng	mdm100	20
7561...	19May2007	11:39:22	mdmf...	udp	domain-udp	mdmfwng	Ns2_Static_Nat	8
7561...	19May2007	11:39:23	mdmf...	udp	domain-udp	cpe-74-65-202-234.nyc....	Ns1_Static_Nat	8
7561...	19May2007	11:39:23	mdmf...	udp	domain-udp	cpe-74-65-202-234.nyc....	Ns1_Static_Nat	8

Gráfico 100

Ejemplo 2: Comprobación de NAT en una máquina de la red 10.10.10.X en la propiedad MIADD.

Esta máquina de la propiedad MIADD tiene como dirección de red 10.10.10.40. En el Web se resuelve como dirección 206.103.146.40.

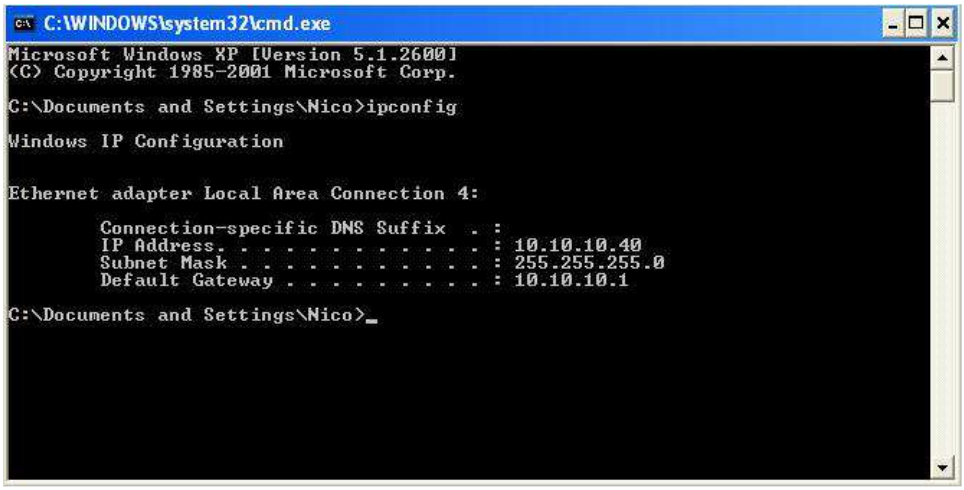


Gráfico 101

Sin embargo al hacer un ping a la dirección 206.103.146.140 desde la misma máquina no tiene respuesta alguna lo cual que primero se realiza un NAT y segundo la dirección real por la cual sale al Internet se encuentra oculta para que esta máquina no sea vulnerable a intrusos.

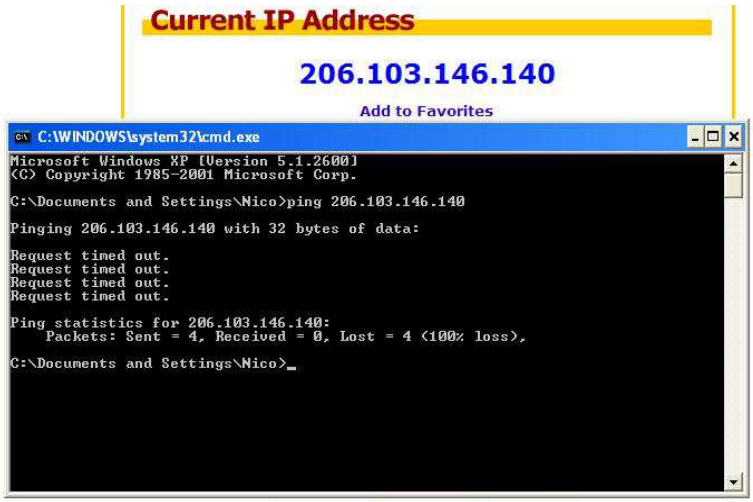


Gráfico 102