

# ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL



**Facultad de Ingeniería en Electricidad y Computación**

**Maestría En Seguridad Informática Aplicada**

"IMPLEMENTACIÓN DE UNA SOLUCIÓN DE SEGURIDAD PERIMETRAL  
CHECK POINT (STANDALONE) PARA UNA PYME"

**EXAMEN DE GRADO (COMPLEXIVO)**

Previa a la obtención del grado de:

**MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA**

JOSÉ LUIS APOLO CALLE

GUAYAQUIL-ECUADOR

AÑO: 2016

## AGRADECIMIENTO

A Dios por la vida y salud para la finalización de este trabajo.

A mi familia por su apoyo y colaboración incondicional para seguir adelante.

A ESPOL y a los profesores por las enseñanzas brindadas que contribuyeron a formarme profesionalmente.

## DEDICATORIA

Dedico este trabajo a mis Padres Elio y Flor María, mis hermanos: Silvia, Carlos y Mary; por su apoyo incondicional y motivación en mis momentos más difíciles, para cumplir mis metas profesionales.

## **TRIBUNAL DE SUSTENTACIÓN**

---

MGS. LENIN FREIRE

DIRECTOR MSIA

---

MGS. ROBERT ANDRADE

PROFESOR DELEGADO

POR LA SUBDECANA DE LA FIEC

---

MGS NESTOR ARREGA

PROFESOR DELEGADO

POR LA SUBDECANA DE LA FIEC

## RESUMEN

Implementar una solución de seguridad informática perimetral para una PYME, haciendo uso de la solución de appliances 4200 de Check Point en modo StandAlone, misma que facilita el control de tráfico, administración y monitoreo en una red de datos.

En el capítulo 1 se abordará generalidades de la problemática de la seguridad informática perimetral, así como también se propone una solución.

En el capítulo 2 se identifica cada uno de los problemas a los cuales se encuentran expuestas las PYMES cuando no poseen soluciones de seguridad perimetral. También se abordará diseños de seguridad perimetral recomendados, basado en una solución Check Point para PYME. Finalmente se mostrará los pasos para implementar una solución de seguridad perimetral.

En el capítulo 3 se enfoca en actividades post-implementación de gran importancia que deben ser tomadas en cuenta; como también medidas a realizar durante mantenimientos preventivos o correctivas de la solución de seguridad perimetral.

En el capítulo 4 se analizarán los resultados obtenidos para garantizar disponibilidad, integridad y confidencialidad de la red PYME; mejoras obtenidas post-implementación, beneficios de la solución, y escalabilidad a futuro.

Finalmente se emitirán las conclusiones y recomendaciones del presente trabajo

## ÍNDICE GENERAL

AGRADECIMIENTO .....	ii
DEDICATORIA .....	iv
TRIBUNAL DE SUSTENTACIÓN .....	iv
RESUMEN .....	v
ÍNDICE GENERAL.....	vii
ABREVIATURAS Y SIMBOLOGÍA .....	xii
ÍNDICE DE FIGURAS.....	xiii
ÍNDICE DE TABLAS .....	xv
INTRODUCCIÓN .....	xvi
CAPÍTULO 1 .....	1
GENERALIDADES .....	1
1.1 DESCRIPCIÓN DEL PROBLEMA.....	1
1.2 SOLUCIÓN PROPUESTA.....	2
CAPÍTULO 2.....	4
IDENTIFICACIÓN DE PROBLEMAS PERIMETRALES EN LA RED .....	4
2.1 MÉTODOS DE ATAQUES PERIMETRALES.....	4
2.1.1 ACCESO NO AUTORIZADO .....	5
2.1.2 APROVECHAMIENTO DE DEBILIDADES CONOCIDAS DE SOFTWARE .....	5
2.1.3 DENEGACIÓN DE SERVICIO .....	6
2.1.4 SUPLANTACIÓN DE IDENTIDAD .....	6

2.1.5 EAVESDROPPING .....	7
2.1.6 CÓDIGO MALICIOSO .....	7
2.2 ARQUITECTURA SIN SEGURIDAD PERIMETRAL .....	8
2.3 UTILIDADES DE UN FIREWALL .....	9
2.3.1 AISLAMIENTO DE INTERNET.....	10
2.3.2 CUELLO DE BOTELLA .....	10
2.3.3 AUDITORÍA Y REGISTRO DE USO .....	10
2.3.4 SEGURIDAD DE CONTENIDOS .....	11
2.3.5 AUTENTICACIÓN .....	12
2.3.6 OCULTAMIENTO DEL RANGO DE DIRECCIONAMIENTO INTERNO DE LA ORGANIZACIÓN .....	12
2.4 DISEÑO DE LA SOLUCION DE SEGURIDAD PERIMETRAL.....	12
2.4.1 CHECK POINT CARACTERÍSTICAS Y FUNCIONALIDADES. ....	13
2.4.1.1 CHECK POINT 4200 APPLIANCE .....	13
2.5 SITUACIÓN INICIAL DE LA RED PYME. ....	15
2.6 SOLUCIÓN PROPUESTA PARA LA PYME. ....	16
2.6.1 COMPONENTE SECURITY GATEWAY .....	17
2.6.1.1 FIREWALL.....	17
2.6.1.2 IPS.....	17
2.6.1.3 IDENTITY AWARENESS .....	18
2.6.1.4 APPLICATION CONTROL .....	18
2.6.1.5 URL FILTER.....	18



2.6.1.6 IPSEC.....	18
2.6.1.7 MOBILE ACCESS .....	19
2.6.1.8 ANTI-VIRUS .....	19
2.6.1.9 ANTI-BOT.....	19
2.6.1.10 ANTI-SPAM.....	19
2.6.2 COMPONENTE SECURITY MANAGEMENT SERVER .....	19
2.6.2.1 NETWORK POLICY MANAGEMENT .....	20
2.6.2.2 LOGGING & STATUS .....	20
2.6.2.3 MONITORING .....	20
2.6.2.4 SMARTREPORTER.....	21
2.6.2.5 PROVISIONING .....	21
2.7 INSTALACIÓN Y CONFIGURACIÓN DEL FIREWALL.....	22
2.7.1 REQUERIMIENTOS PARA LA INSTALACIÓN.....	23
2.7.2 INSTALACIÓN STANDALONE .....	23
2.7.2.1 PROCEDIMIENTO DE INSTALACIÓN .....	24
2.7.2.2 CONFIGURACIONES EN SMARTCONSOLE .....	26
2.8 CONFIGURACIÓN DE MODULOS DEL APPLIANCE.....	30
2.8.1 POLÍTICAS DE SEGURIDAD .....	30
2.8.2 APPLICATION CONTROL & URL FILTERING .....	32
2.8.3 IPS.....	33
2.8.4 THREAT PREVENTION.....	33
2.8.5 ANTI-SPAM & MAIL .....	34

2.8.6 IPsec VPN .....	35
2.9 CONSOLAS DE MONITOREO EN SMARTDASHBOARD .....	36
2.9.1 SMARTVIEW TRACKER.....	36
2.9.2 SMARTEVENT .....	37
2.9.3 SMARTUPDATE .....	38
2.9.4 SMARTREPORTER .....	39
CAPÍTULO 3.....	41
TAREAS POST IMPLEMENTACION.....	41
3.1 RUTINAS DE MANTENIMIENTO.....	41
3.1.1 ENCENDIDO Y APAGADO DEL EQUIPO .....	41
3.1.1.1 APAGADO MEDIANTE INTERFAZ WEB.....	42
3.1.1.2 APAGADO MEDIANTE CONSOLA.....	43
3.2 CREACIÓN DE RESPALDOS.....	44
3.3 BORRADO DE LOGS .....	45
3.4 UPGRADE DE OS.....	46
CAPÍTULO 4.....	47
RESULTADOS.....	47
4.1 ANÁLISIS DE RESULTADOS .....	47
4.1.1 DISPONIBILIDAD.....	47
4.1.2 INTEGRIDAD .....	48
4.1.3 CONFIDENCIALIDAD .....	49
CONCLUSIONES Y RECOMENDACIONES.....	51

BIBLIOGRAFÍA.....	54
APÉNDICE.....	55

## ABREVIATURAS Y SIMBOLOGÍA

<b>BSD</b>	Berkeley Software Distribution
<b>DOS</b>	Denial of Service
<b>Gbps</b>	Gigabits por segundo
<b>HTTPS</b>	Hypertext Transfer Protocol Secure
<b>IP</b>	Internet Protocol
<b>IPS</b>	Intrusion Prevention system
<b>NAT</b>	Network Address Translation
<b>NFS</b>	Network File System
<b>OS</b>	Operating System
<b>SG</b>	Security Gateway
<b>SM</b>	Security Manager
<b>SPU</b>	Secure Power Units

## ÍNDICE DE FIGURAS

Figura 2.1 Diagrama de red insegura .....	8
Figura 2.2 Esquema básico de un firewall .....	9
Figura 2.3 Appliance 4200 .....	13
Figura 2.4 Esquema de red inicial de la PYME .....	16
Figura 2.5 Esquema de red propuesto para la PYME.....	22
Figura 2.6 Standalone deployment .....	23
Figura 2.7 Pantalla de ingreso SmartDashboard .....	26
Figura 2.8 Pantalla Smartconsole .....	27
Figura 2.9 Pantalla gateway PYME .....	28
Figura 2.10 Pantalla componente security .....	29
Figura 2.11 Pantalla componente management .....	30
Figura 2.12 Pantalla rule base firewall .....	31
Figura 2.13 Pantalla políticas de application control y url filter .....	32
Figura 2.14 Pantalla IPS .....	33
Figura 2.15 Pantalla threat prevention .....	34
Figura 2.16 Pantalla anti-spam .....	35
Figura 2.17 Pantalla IPSEC VPN.....	35
Figura 2.18 Pantalla Smartview tracker .....	36
Figura 2.19 Pantalla SmartView tracker – detalle .....	37
Figura 2.20 Pantalla Smartevent.....	38

Figura 2.21 Pantalla SmartUpdate.....	39
Figura 2.22 Pantalla SmartReporte.....	40
Figura 3.1 Pantalla GAIA Portal .....	42
Figura 3.2 Pantalla apagado de appliance.....	43
Figura 3.3 Pantalla apagado por consola .....	43
Figura 3.4 Pantalla apagado en modo experto .....	44
Figura 3.5 Pantalla para sacar backup .....	45
Figura 3.6 Pantalla de Logs .....	45
Figura 3.7 Pantalla para hacer upgrades del OS.....	46

## ÍNDICE DE TABLAS

Tabla 1. Blades disponibles para el Appliance 4200.....	14
---	----

## INTRODUCCIÓN

Hoy en día, la gran mayoría de avances tecnológicos y de comunicación y el funcionamiento de las mismas a través del protocolo IP, ha permitido el surgimiento de nuevos ataques y modalidades delictivas que han transformado al internet y las tecnologías informáticas en aspectos sumamente peligrosas para cualquier tipo de organización que tenga equipos conectados a la World Wide Web.

A diario se descubren nuevos puntos débiles, nuevas formas de ataque y, por lo general, son pocos los responsables de IT que comprenden la importancia que tiene la seguridad y cómo pueden mitigar el grave problema que existe detrás de vulnerabilidades que permiten a un atacante, violar la seguridad de un entorno y cometer delitos en función de los datos robados [1].

En esta tesis, abordaremos varios puntos relevantes en cuanto a la seguridad perimetral: Ataques más comunes que existen en el perímetro de una red,



como poder identificarlos, como poder contrarrestarlos, y como implementar una solución perimetral óptima en una red PYME.

La solución brindada en el presente documento se basa en una solución de Check Point, contaremos con un appliance Check Point 4200 que operará en modo StandAlone (Operación Centralizada) en el cual se habilitarán los blades de seguridad y administración y reportería.

# **CAPÍTULO 1**

## **GENERALIDADES**

### **1.1 DESCRIPCIÓN DEL PROBLEMA**

Hoy en día, aún existen pequeñas y medianas empresas que no tienen soluciones de seguridad perimetral IT en sus redes, observan la necesidad de herramientas que les facilite la administración, control y monitoreo del tráfico entre sus redes de datos LAN, WAN, DMZ; sin embargo, pocas son las PYMEs que se atreven a abordar este nuevo paradigma tecnológico sin que existan pérdidas cuantiosas de dinero por los delitos informáticos.

La no implementación de soluciones de seguridad perimetral, hace que las PYMEs se encuentren expuestas a ser blanco de ataques cibernéticos (Cyber attacks); entre los más conocidos: Defacement, phishing, DoS, Spyware, Malware, puerta trasera, adware, y más.

Los ataques cibernéticos son originados; debido a, que existen muchas vulnerabilidades en las PYMES; por ejemplo: Uso de tecnología obsoleta, bajo presupuesto, falta de conocimiento técnico y de nuevas soluciones de seguridad IT, o simplemente falta de interés en la seguridad IT.

## **1.2 SOLUCIÓN PROPUESTA**

La solución que se propone contempla la implementación de una solución de seguridad perimetral de próxima generación, dada por el fabricante Check Point. La misma fue implementada en una PYME en el Ecuador y puede tomarse como base para aplicarse en varias PYMES, ya que son compañías que buscan soluciones de seguridad IT bastante eficientes, granulares, escalables, fácil gestión, y por su puesto económicamente alcanzables a su presupuesto.

En resumen; la solución de Seguridad Perimetral Check Point contempla los siguientes componentes (hardware) y cada uno con su respectivo blade (servicio) descritos a continuación.

- 1 Appliances 4200.- Realizará funciones propias de un Firewall perimetral, administración y control, lo blades activos tenemos:
  - Firewall
  - IPSec
  - Mobile Access
  - IPS
  - Anti-bot
  - Anti-virus
  - Anti-Spam & Email Security
  - URI Filter
  - Application Control
  - Security Management
  - Network Policy Management
  - Logging & Status
  - Provisioning

## **CAPÍTULO 2**

### **IDENTIFICACIÓN DE PROBLEMAS PERIMETRALES EN LA RED**

#### **2.1 MÉTODOS DE ATAQUES PERIMETRALES**

Un ataque informático consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; a fin de obtener un beneficio, por lo general de índole económico, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización [2].

Como administradores de red, es importante entender la naturaleza de los posibles ataques a la seguridad informática perimetral. A continuación, se

describirá de manera resumida los tipos de ataques más importantes y posteriormente se indicará cómo actuar ante estas situaciones.

### **2.1.1 ACCESO NO AUTORIZADO**

Esto simplemente quiere decir que, personas que no deberían utilizar los servicios de su computadora son capaces de conectarse y utilizarlos. Por ejemplo, personas de fuera de su compañía podrían intentar conectarse a la máquina con las cuentas de su compañía o a su servidor de NFS.

### **2.1.2 APROVECHAMIENTO DE DEBILIDADES CONOCIDAS DE SOFTWARE**

Algunos programas y servicios de red no fueron diseñados originalmente teniendo en cuenta una elevada seguridad y son inherentemente vulnerables a los ataques. Los servicios remotos del tipo BSD (rlogin, rexec, etc) constituyen un ejemplo.

### **2.1.3 DENEGACIÓN DE SERVICIO**

Los ataques de denegación de servicio causan que el servicio o programa deje de funcionar o impide que otros hagan uso de ese servicio o programa. Estos ataques pueden ser realizados al nivel de red enviando datagramas cuidadosamente preparados y malintencionados de tal forma que puedan causar que las conexiones de red fallen. También pueden realizarse a nivel de aplicación, donde órdenes cuidadosamente construidas se envían contra un programa para tratar que se vuelva muy ocupado o que pare su funcionamiento.

### **2.1.4 SUPLANTACIÓN DE IDENTIDAD**

Este tipo de ataque causa que un 'host' o aplicación simule las acciones de otro. Típicamente, el atacante se hace pasar por un 'host' inocente siguiendo el rastro de las direcciones IP contenidas en los paquetes de red. Por ejemplo, un 'exploit' bien documentado del servicio de tipo BSD rlogin puede utilizar esta técnica para simular una conexión de TCP desde otro 'host' prediciendo los números de secuencia de TCP.

### **2.1.5 EAVESDROPPING**

Éste es el método de ataque más simple. Un 'host' se configura para "escuchar" y capturar los datos no destinados a él. Programas de fisgoneo cuidadosamente escritos pueden obtener los nombres de usuario y sus contraseñas a partir de las conexiones de red con ingresos de usuarios en el sistema. Redes de difusión como las de tipo Ethernet son especialmente vulnerables a este tipo de ataques.

### **2.1.6 CÓDIGO MALICIOSO**

Códigos maliciosos, o malware, constituyen también una de las principales amenazas de seguridad para cualquier Institución u Organizaciones y aunque parezca un tema trivial, suele ser motivo de importantes pérdidas económicas.

Esta amenaza se refiere a programas que causan algún tipo de daño o anomalía en el sistema informático. Dentro de esta categoría se incluyen los programas troyanos, gusanos, virus informáticos, spyware, backdoors, rootkits, keyloggers, entre otros.



## 2.2 ARQUITECTURA SIN SEGURIDAD PERIMETRAL

Una red que es insegura en el perímetro denota las siguientes características [3]:

- Red plana sin segmentar.
- Publicación de servicios internos: base de datos, mail, aplicaciones.
- No hay elementos de monitorización.
- No se filtra tráfico de entrada ni salida.
- No se verifica malware o spam en el correo electrónico.
- Cliente remoto accede directamente a los servicios

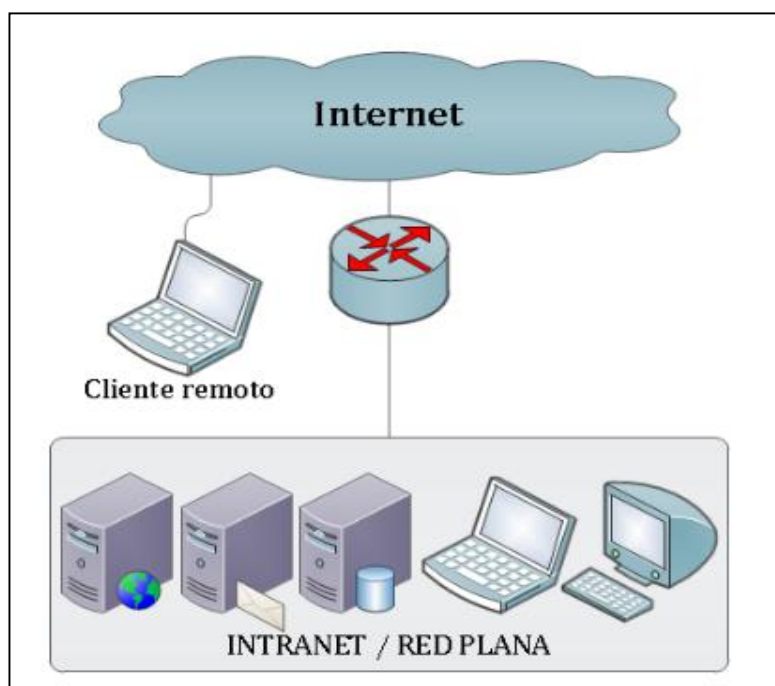


Figura 2.1 Diagrama de Red Insegura

### 2.3 UTILIDADES DE UN FIREWALL

Un cortafuegos o firewall es un sistema de defensa basado en el hecho de que todo el tráfico de entrada o salida a la red debe pasar obligatoriamente por un sistema de seguridad capaz de autorizar, denegar, y registrar de todo aquello que ocurre, según lo implementado con las políticas de control de acceso entre varias redes [4].

Este sistema, controla la comunicación desde el exterior hacia un host en la red interna o viceversa. Actúa a base de normas que establece el administrador de seguridad o, en su defecto, el administrador de red o el usuario final.

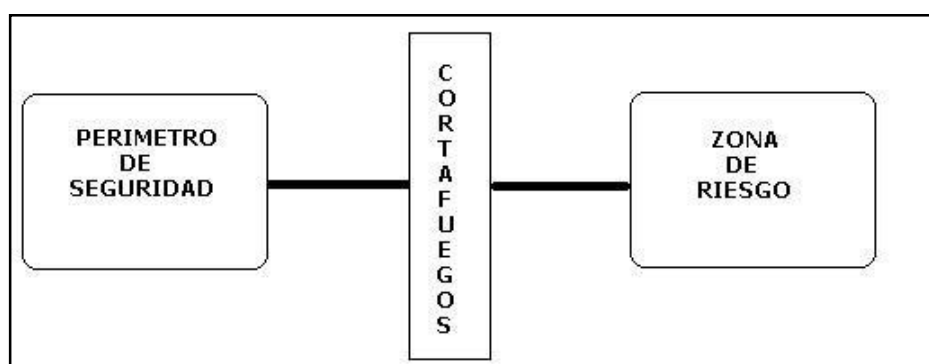


Figura 2.2 Esquema básico de un firewall

Entre las principales utilidades del firewall tenemos.

### **2.3.1 AISLAMIENTO DE INTERNET**

El firewall restringe el acceso hacia/desde la red interna sólo a ciertos servicios, a la vez que analiza todo el tráfico que pasa por el mismo.

### **2.3.2 CUELLO DE BOTELLA**

Busca concentrar la administración y monitoreo de la seguridad de la red en un solo punto. Mantiene a los atacantes y peligros alejados de la red interna, prohíbe en los dos sentidos servicios susceptibles a ataques y proporciona protección ante algunos tipos de ataques basados en el "enrutamiento" de paquetes

### **2.3.3 AUDITORÍA Y REGISTRO DE USO**

Constituye un buen lugar donde recopilar información sobre el uso de la red. En su calidad de punto único de acceso, el firewall puede registrar toda la actividad entre la red exterior y la interior. Con todos estos datos, el administrador puede posteriormente estudiar estadísticamente el tipo de tráfico, las horas de mayor carga de trabajo,

el ancho de banda consumido y, por supuesto, todos los intentos de intrusión o las pistas dejadas por un atacante

#### **2.3.4 SEGURIDAD DE CONTENIDOS**

Una característica incorporada por un número cada vez mayor de cortafuegos es la inspección antivirus del material transmitido a través de determinados servicios. Presenta el problema de consumir muchos recursos, ya que se deben descomprimir o decodificar ciertos ficheros (ZIP, MIME, Unicode), escanearlos y tomar una decisión antes de retransmitirlos dentro de la red. Algunos cortafuegos bloquean también programas en Java, controles ActiveX, guiones en JavaScript o en VisualBasic Script, que pueden ser potencialmente peligrosos, bien formando parte del contenido de un mensaje de correo o de una página web

### **2.3.5 AUTENTICACIÓN**

Algunos firewalls permiten autenticarse utilizando métodos sofisticados, basados en tarjetas inteligentes, contraseñas de un solo uso, llaves hardware, etc.

### **2.3.6 OCULTAMIENTO DEL RANGO DE DIRECCIONAMIENTO INTERNO DE LA ORGANIZACIÓN**

Es lo que se conoce como NAT (Network Address Translation) cuya función es realizar una traducción de las direcciones de red, de modo que las direcciones de las máquinas internas quedan ocultas para el exterior.

## **2.4 DISEÑO DE LA SOLUCIÓN DE SEGURIDAD PERIMETRAL**

Hoy en día existen varios fabricantes que han desarrollado firewalls de protección de redes en el perímetro. En el presente trabajo nos enfocaremos en una solución dada por Check Point y que fue implementada en una PYME en Ecuador.

## 2.4.1 CHECK POINT CARACTERÍSTICAS Y FUNCIONALIDADES.

Los equipos que se utilizaron para implementar en la PYME fueron los siguientes:

- Check Point Appliance 4200
- Laptop

### 2.4.1.1 CHECK POINT 4200 APPLIANCE

El appliance 4200 es ideal para Pymes, posee características como: 3 Gbps de rendimiento del firewall, 2 Gbps de desempeño del IPS y 114 SPUs además de una variedad de opciones de conectividad en cobre y fibra óptica. Cuenta con almacenamiento de 250 Gb y 4 puertos con flexibilidad a sumar 4 puertos más. [5].



Figura 2.3 Appliance 4200

1. Slot de expansión para una tarjeta de red
2. Puerto de consola
3. Fuente de poder AC
4. Puertos de red 10/100/1000 Base-T
5. Puertos USB para instalación usando ISO
6. Display LCD Grafico

En el appliance se pueden habilitar varios blades dependiendo la necesidad del cliente.

<b>GATEWAY SOFTWARE BLADES</b>				
	<b>FW</b>	<b>NGFW</b>	<b>NGDP</b>	<b>NGTP</b>
Firewall	■	■	■	■
IPsec VPN	■	■	■	■
Mobile Access (5 users)	■	■	■	■
Advanced Networking & Clustering	■	■	■	■
Identity Awareness	■	■	■	■
IPS	*	■	■	■
Application Control	*	■	■	■
Data Loss Prevention	*	*	■	*
URL Filtering	*	*	*	■
Antivirus	*	*	*	■
Anti-spam	*	*	*	■
Anti-Bot	*	*	*	■
* Optional				

Tabla 1 Blades disponibles para el Appliance 4200

## 2.5 SITUACIÓN INICIAL DE LA RED PYME.

Posterior a levantamientos de información realizados con el administrador de red de la PYME, se logró identificar lo siguiente:

- La red consta de aproximadamente 200 usuarios.
- No tenían un dispositivo de seguridad perimetral en la red; es decir, la red se encontraba expuesta a ataques desde el internet.
- Poseían servicios publicados en la red a través de direcciones IP's públicas fáciles de identificar.
- La red se encontraba segmentada internamente por VLANs que se ven entre sí; es decir, tampoco tenían listas de acceso entre redes, permitiendo que cualquier usuario interno pueda acceder a bases de datos y demás servidores de la compañía.
- Para acceder desde el exterior hacia la red interna, utilizaban aplicativos de acceso remotos libres.
- En conversaciones con el administrador de la red indicaba que tenían un sin número de ataques imposibles de identificar.
- En varias ocasiones la red colapsaba sin saber que sucedió.



La PYME tenía el siguiente esquema de red.

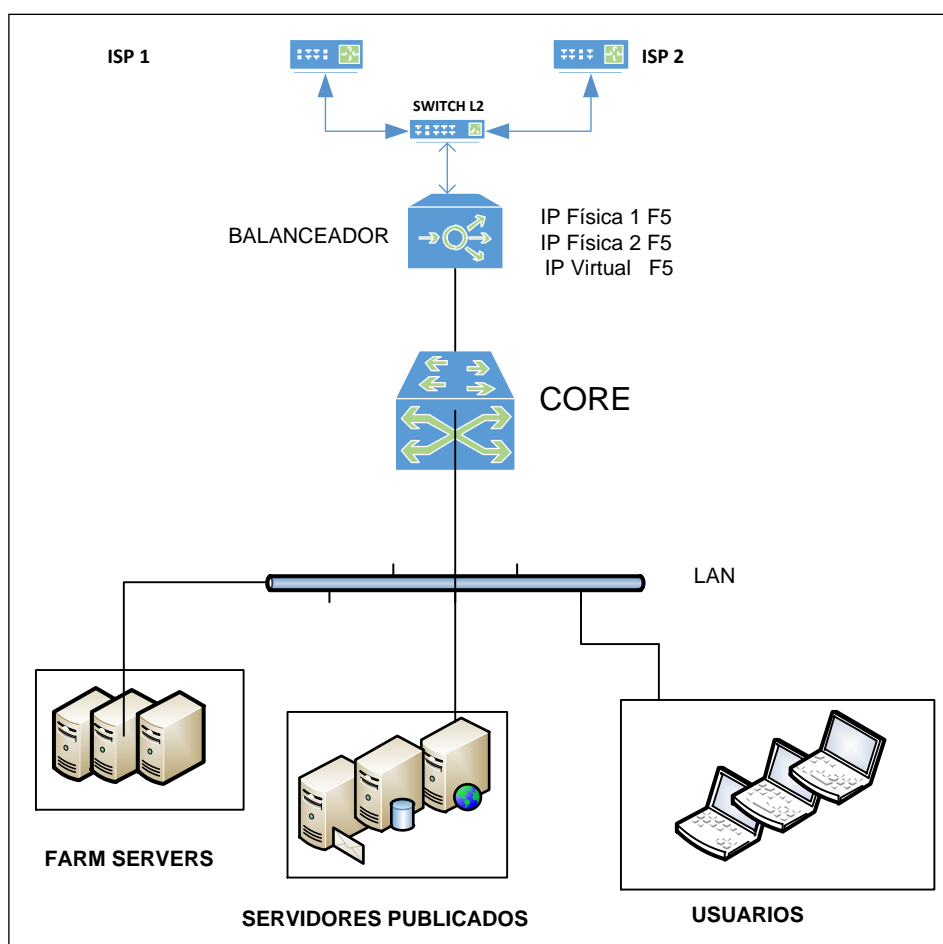


Figura 2.4 Esquema de red inicial de la PYME

## 2.6 SOLUCIÓN PROPUESTA PARA LA PYME.

Se instalará y configurará un equipo Appliance Check Point 4200 mismo que tendrá dos componentes instalados:

- Security Gateway
- Security Management Server

En el componente Security Gateway se habilitarán los siguientes módulos/blades, mismos que servirán para contrarrestar todas las vulnerabilidades que tiene la PYME.

### **2.6.1 COMPONENTE SECURITY GATEWAY**

Este componente realiza las funciones de ejecución de políticas globales en el appliance; es decir, ejecuta las políticas de redes, control de aplicaciones, NAT, antivirus, anti-bot entre otros, que el componente Security Management envía o tiene configuradas. En nuestro caso, este componente tendrá habilitado los siguientes módulos o blades.

#### **2.6.1.1 FIREWALL**

Control de acceso entre redes internas / externas

#### **2.6.1.2 IPS**

Habilita las funcionalidades del Intrusion Prevention System del appliance.

### **2.6.1.3 IDENTITY AWARENESS**

Integración con MS Active Directory, a fin de que las protecciones se asocien a los usuarios y no a direcciones IP

### **2.6.1.4 APPLICATION CONTROL**

Permite la integración con MS Active Directory, a fin de que las protecciones se asocien a los usuarios y no a direcciones IP

### **2.6.1.5 URL FILTER**

Control de acceso a URLs mediante una base de datos de sitios web categorizados.

### **2.6.1.6 IPSEC**

Habilita las VPN site to site o de Acceso remoto

### **2.6.1.7 MOBILE ACCESS**

Habilita el blade de VPN SSL y a través de dispositivos móviles

### **2.6.1.8 ANTI-VIRUS**

Habilita el antivirus perimetral del appliance.

### **2.6.1.9 ANTI-BOT**

Blade de antibot Perimetral

### **2.6.1.10 ANTI-SPAM**

Solución de antispam perimetral

## **2.6.2 COMPONENTE SECURITY MANAGEMENT SERVER**

El componente security management facilita la administración de las políticas de seguridad y registros o eventos suscitados en el firewall.

Para nuestra propuesta de seguridad perimetral se habilitaron los siguientes módulos.

#### **2.6.2.1 NETWORK POLICY MANAGEMENT**

Facilita la administración de las políticas de seguridad de manera comprensiva, unificando todas las funcionalidades en una sola consola.

#### **2.6.2.2 LOGGING & STATUS**

Registra todas las actividades por Gateway, túneles o usuarios de manera completa y comprensiva adicionalmente utiliza gráficos.

#### **2.6.2.3 MONITORING**

Muestra un gráfico completo de la red y el desempeño del equipo, y habilita tener respuestas rápidas a cambios según patrones o eventos de seguridad.

#### **2.6.2.4 SMARTREPORTER**

Recoge gran cantidad de eventos por políticas de seguridad y dispositivos en la red.

#### **2.6.2.5 PROVISIONING**

Administra la configuración y centraliza las políticas del dispositivo

Posterior a las funcionalidades propuestas a activar en cada componente Check Point, a continuación, se mostrará el esquema de red propuesto para la PYME.

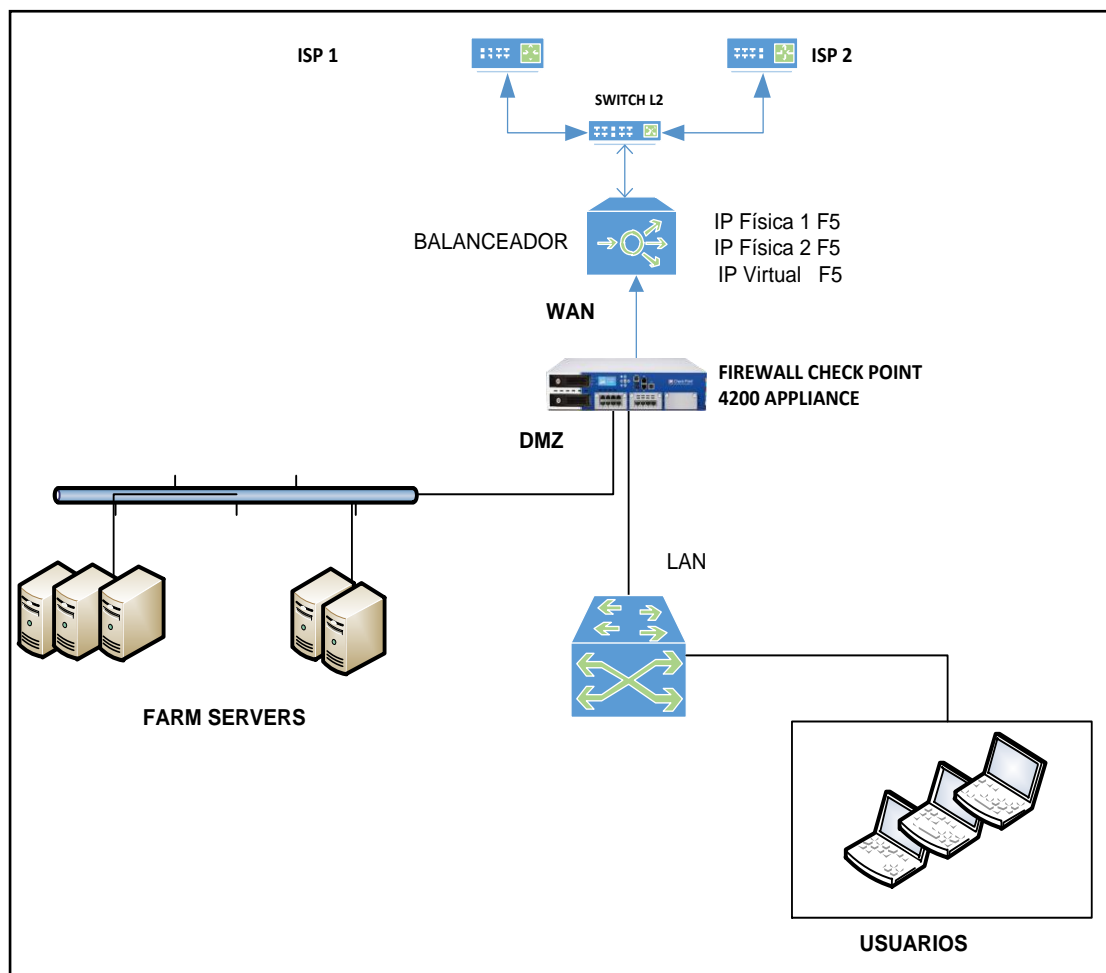


Figura 2.5 Esquema de red propuesto para la PYME

## 2.7 INSTALACIÓN Y CONFIGURACIÓN DEL FIREWALL.

La solución comprende la instalación en modo StandAlone del dispositivo. Cabe recalcar que el appliances viene pre configurado desde fábrica por lo que la instalación es bastante sencilla, se recomienda antes de empezar la instalación tener listo el direccionamiento IP a poner al equipo.

## 2.7.1 REQUERIMIENTOS PARA LA INSTALACIÓN

Para realizar la instalación se requiere lo siguiente:

- 1 Appliance Check Point 4200, con Sistema Operativo GAIA versión R77.30 hasta ahora el más estable.
- Direccionamiento IP para el Appliance
- Licenciamiento para habilitar los módulos. En este caso se propuso habilitar la Licencia Next Generation Threat Prevention

## 2.7.2 INSTALACIÓN STANDALONE

Esta instalación consiste en implementar un firewall y su administración en un solo appliance; es decir, utilizando la nomenclatura Check Point, el Security Management Server y el Security Gateway están instalados en el mismo equipo.




	Item	Description
	1	Standalone computer
		Security Gateway component
		Security Management Server component

Figura 2.6 StandAlone Deployment



### 2.7.2.1 PROCEDIMIENTO DE INSTALACIÓN

Para realizar la instalación se procede de la siguiente manera [6]:

- Se conecta una laptop al appliance a través de la interfaz de administración, la misma viene con una ip por default 192.168.1.1.
- Conectarse a la máquina del Portal Gaia utilizando la siguiente dirección: <https://192.168.1.1> y con las siguientes credenciales usuario: admin; password:admin, clic login
- Click en 'next' en la página de bienvenida y se configura los siguientes detalles.
  - En la sección setup, escoger las opciones de implementación Quick Standalone setup fo GAIA y clic en siguiente.
  - En el quick setup se configura lo siguiente dirección IP de la interface de administración.
  - Autenticación; nuevo password, confirme el nuevo password, mismo que se utilizará para acceder al GAIA OS como a la cuenta admin del security management server
  - Dirección IP de la interface externa para conectar hacia el internet
  - Configuraciones de redes: Default Gateway, dns.
  - Escoger la topología: Modo monitor, modo brigde
  - Para verificar conectividad, dar clic en test connectivity

- Clic en 'next' y posteriormente clic en 'finish' para empezar el proceso de configuración.

Al finalizar la configuración, el equipo se reiniciará, el proceso de iniciación de los servicios trabajará en background, y durante estos minutos en caso de acceder por smartconsole solo se tendrá accesos de lectura. Sino tiene el instalador del smartconsole se lo debe descargar desde el mismo appliance dirigiéndose al explorador y apuntando la siguiente dirección [https:// <management\\_ip\\_address>](https://<management_ip_address>), en la pestaña 'overview' clic en download now.

Posteriormente instalamos el smartconsole al computador desde el cual desee manejar la administración; para esto buscamos ingresamos al smartdashboard.



Figura 2.7 Pantalla de ingreso SmartDashboard

Utilizamos las credenciales configuradas en la parte inicial

### 2.7.2.2 CONFIGURACIONES EN SMARTCONSOLE

La pantalla smartconsole facilita la administración de todas las bondades del firewall.

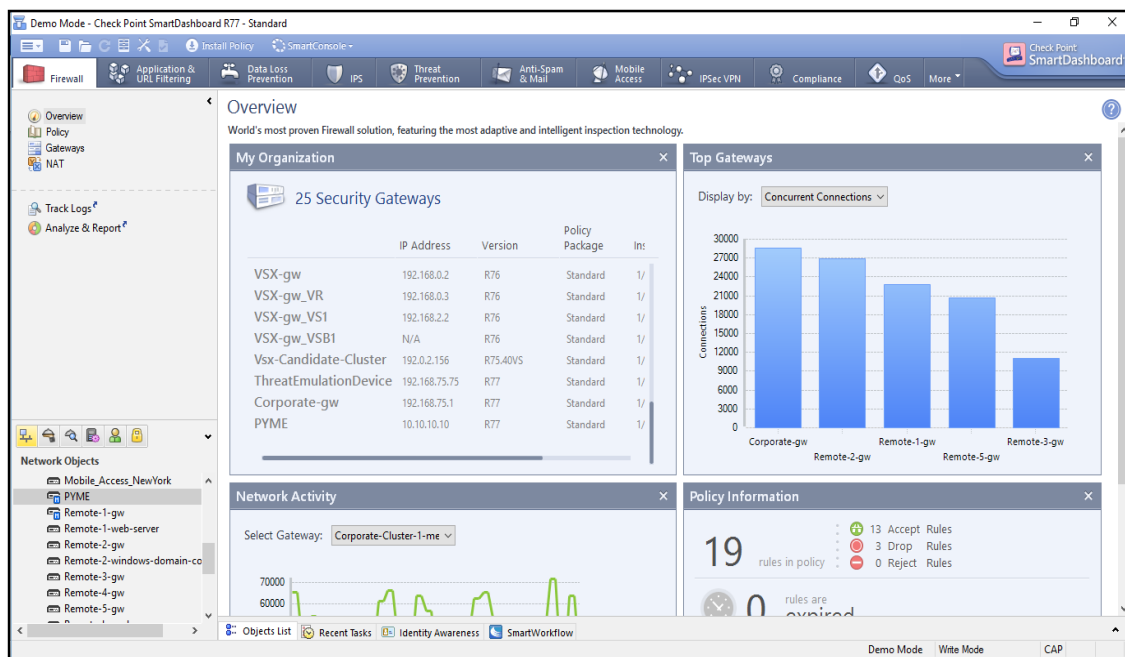


Figura 2.8 Pantalla Smartconsole

En la pantalla principal del smartconsole, específicamente en network objects ubicado en la parte inferior izquierda veremos el objeto del firewall. Y damos doble clic para empezar la configuración y habilitación de módulos. Logrando la siguiente pantalla.

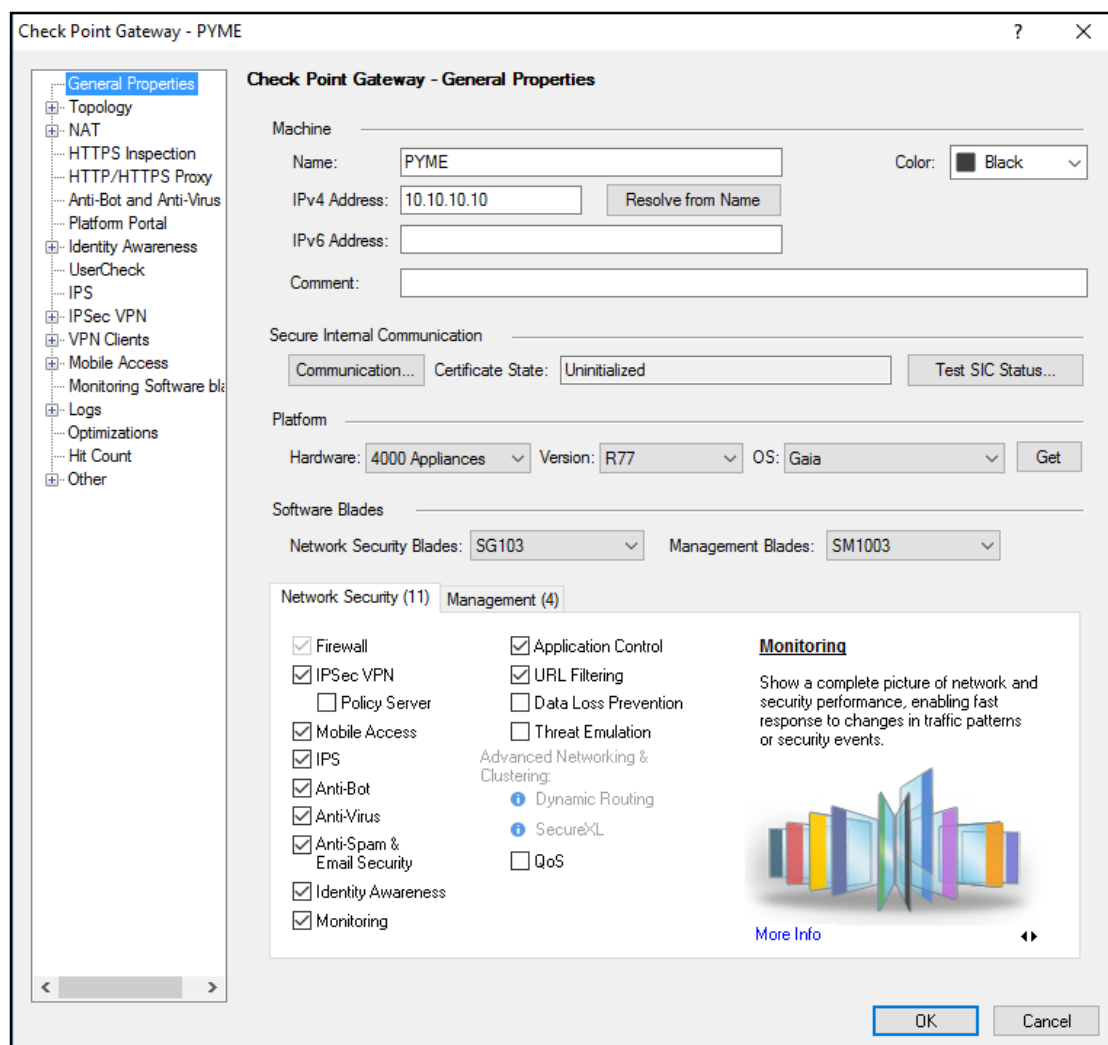


Figura 2.9 Pantalla gateway PYME

Según lo mostrado en la Figura 2.9, seleccionamos los módulos/blades que utilizaremos en el componente security gateway, siendo estos:

- Firewall
- IPSec
- Mobile Access
- IPS
- Anti-bot

- Anti-virus
- Anti-Spam & Email Security
- Identity Awareness
- Monitoring
- URI Filter
- Application Control

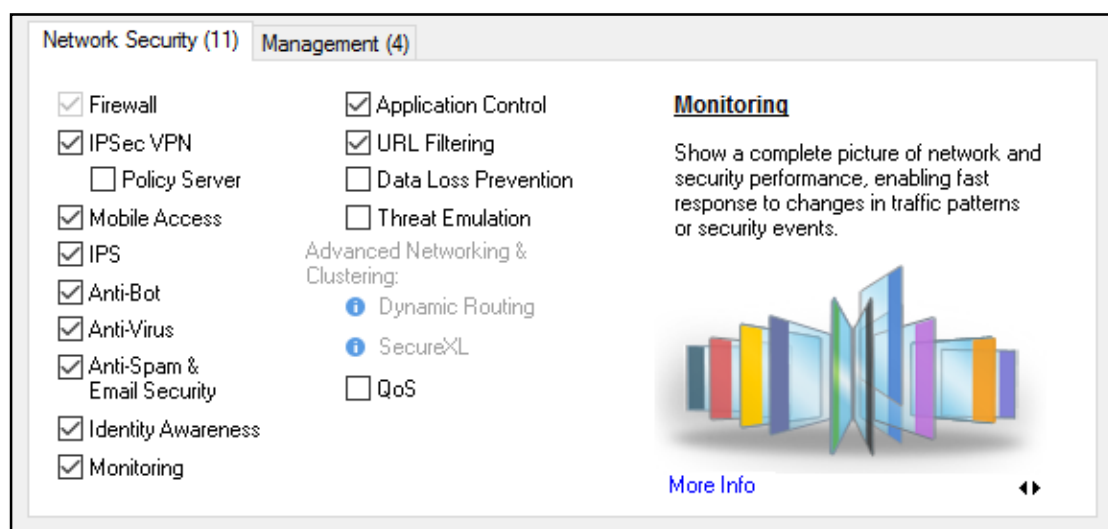


Figura 2.10 Pantalla componente security

Según lo mostrado en la Figura 2.9, seleccionamos los módulos/blades que utilizaremos en el componente security management, siendo estos:

- Network policy management
- Logging & status
- Monitoring
- Provisioning
- SmartReporter

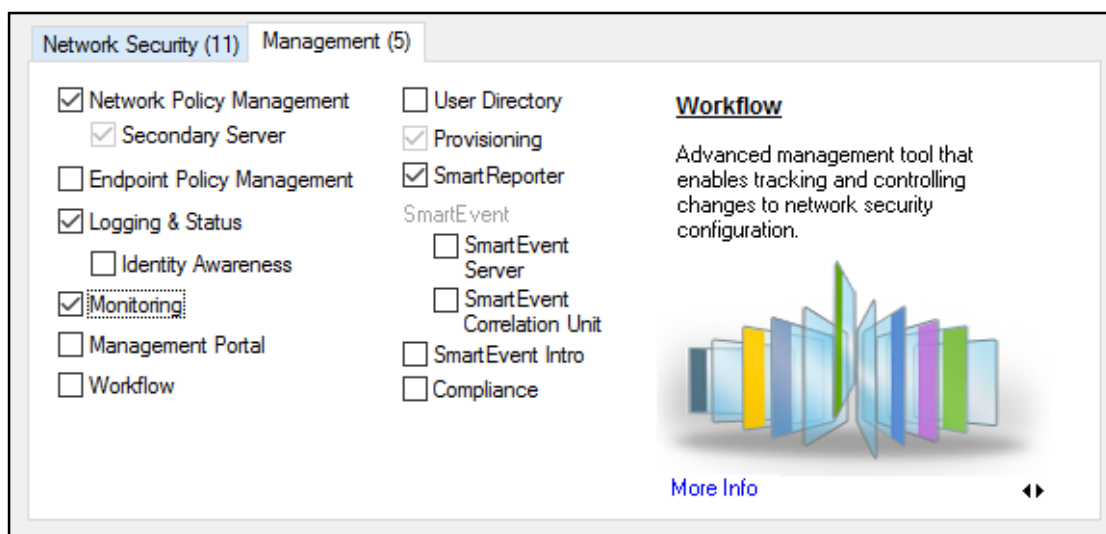


Figura 2.11 Pantalla componente management

## 2.8 CONFIGURACIÓN DE MODULOS DEL APPLIANCE

A través del smartdashboard configuramos cada uno de los módulos activos

### 2.8.1 POLÍTICAS DE SEGURIDAD

El grupo de Políticas dentro del rule base se recomienda realizarlo en un determinado orden, de esta manera facilitamos la administración

- Reglas de Comunicación hacia el firewall Check Point
- Reglas de acceso por VPNs
- Reglas de acceso a sitios específicos y de NAT

- Reglas de acceso basadas en identidad
- Reglas comunes de Firewalls
- Regla de Cleanup

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On	Time
<b>Limit Access to Gateways Rule (Rule 1)</b>										
1	697K	Stealth	Corporate-inte	GW-group	Any Traffic	Any	drop	Alert	Policy Targets	Any
<b>VPN Access Rules (Rules 2-3)</b>										
2	1M	Site to site VPN	Any	Any	All_GwToGw	CIFS, https, smtp	accept	Log	Policy Targets	Any
3	224K	Web server	L2TP-vpn-user@Customers@Ar	Remote-1-web	Any Traffic	http	accept	Log	Policy Targets	Any
<b>Rules for Specific Sites (Rules 4-6)</b>										
4	6M	Outbound HTTP	Remote-2-inter	Any	Any Traffic	http	Client Auth	Log	Remote-2-gw	Any
5	511K	Critical subnet	Corporate-inte	Corporate-fina Corporate-hr-n	Any Traffic	Any	accept	Log	Corporate-gw	Any
6	26K	Tech support	Tech-Support	Remote-1-web	Any Traffic	http	accept	Alert	Remote-1-gw	Any
<b>Identity Based Access (Rules 7-8)</b>										
7	1M	HR Server Allow	John_Adams_R HR_Partners_M	HR_Server	Any Traffic	Any	accept (display ca)	Log	Corporate-gw Remote-1-gw	Any
8	19K	Internet Access	Guests All_Domain_Us	inet_http_prox	Any Traffic	HTTP_and_HTTP	accept (display ca)	Log	Corporate-gw Remote-1-gw	Any
<b>Common Rules - All Sites (Rules 9-11)</b>										
9	615K	Terminal server	Corporate-inte	Any	Any Traffic	Any	Session Auth	Log	Corporate-gw	Any

Figura 2.12 Pantalla rule base firewall



## 2.8.2 APPLICATION CONTROL & URL FILTERING

A diferencia de las reglas de Firewall, este blade debe ser usado para restringir el acceso de usuarios al internet, también puede usarse para hacer restricciones por IP o por roles (usuarios) como sea el caso.

No.	Hits	Name	Source	Destination	Applications/Sites	Action	Track	Install On	Time	Comme
1	2M	Allow HR to browse MyHR.com site	HR	Internet	MyHR.com	Inform Inform Sensitive... Once a day	Log	All	Any	
2	217	Block sites which may cause liability	Any	Internet	Potential_liability	Block Blocked Message	Log	All	Any	
3	401	Block High risk applications	Any	Internet	High Risk	Block High Risk Block	Log	All	Any	
4	0	Block malwares	Any	Internet	Anonymizer	Block Blocked Message	Log	All	Any	
5	66K	Allow TeamViewer application for specific user - tirk# #88721	John_Adams_Role	Any	TeamViewer	Allow	Log	All	Any	
6	12K	Allow remote admin for IT Dept only	IT_Department	Any	Radmin	Allow	Log	All	Work-Hours	
7	813	Allow Facebook only to HR	HR	Internet	Facebook	Allow Download_1Gbps Down: 1 Gbps	Log	All	Any	
8	3M	Allow streaming only for Marketing, and verify access	Marketing	Internet	Vimeo YouTube	Ask Company Policy Once a day	Log	All	Any	

Figura 2.13 Pantalla políticas de application control y url filter

### 2.8.3 IPS

En este blade solo se debe configurar el perfil, en este caso está configurado el perfil por defecto, se puede usar el perfil recomendado, pero se debe tener en cuenta que es un modo más agresivo, por lo cual en ciertas ocasiones es necesario personalizar el perfil para que no bloquee falsos positivos.

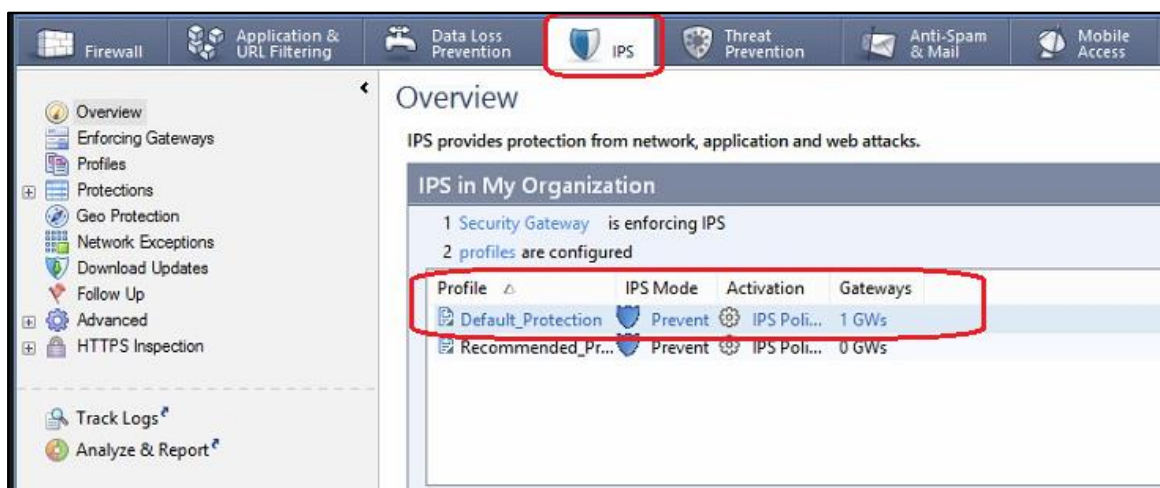


Figura 2.14 Pantalla IPS

### 2.8.4 THREAT PREVENTION

En esta pestaña están consolidados los blades de Anti-Bot, Anti-virus y Threat Emulation. En este caso los blades activos de Anti-Bot y Anti-virus están activos, por lo cual aparecen en esta ok, se recomienda

siempre estar pendiente de que las firmas de anti-Bot y anti-virus estén actualizadas.

The screenshot displays the 'Gateways' management console. On the left, a table lists four gateways: Remote-3-gw, ThreatEmulationDevice, Corporate-gw, and PYME. The PYME gateway is selected, and its configuration details are shown on the right. The configuration includes status checks for Anti-Bot, Anti-Virus, and Threat Emulation, all of which are up to date as of 1/10/2016. It also shows subscription status for Anti-Bot, Anti-Spam, Anti-Virus, and Threat Emulation, all of which are up to date. Finally, it displays threat emulation statistics: 2 files in the emulation queue, 7M files emulated (cloud), and 9M files scanned (total).

Gateway	IP Address	Anti-Bot	Anti-Virus	Threat Emulation
Remote-3-gw	10.75.25.1	Disabled	Disabled	Enabled
ThreatEmulationDevice	192.168.75.75	Disabled	Disabled	Enabled
Corporate-gw	192.168.75.1	Enabled	Enabled	Enabled
PYME	10.10.10.10	Enabled	Enabled	Enabled

**PYME**

**Update Status**

- Anti-Bot: Gateway is up to date. 1/10/2016
- Anti-Virus: Gateway is up to date. 1/10/2016
- Threat Emulation: Gateway is up to date. 1/10/2016

**Subscription Status**

- Anti-Bot: Contract is up to date.
- Anti-Spam: Contract is up to date.
- Anti-Virus: Contract is up to date.
- Threat Emulation: Contract is up to date.

**Threat Emulation**

- Analysis Location: This gateway
- Files In Emulation Queue: 2
- Files Emulated (Cloud): 7M
- Files Scanned (Total): 9M

Figura 2.15 Pantalla threat prevention

## 2.8.5 ANTI-SPAM & MAIL

En esta pestaña se encuentra la configuración del blade de Anti-Spam. Para este caso en particular el servidor de correo se encuentra en Internet, por lo cual al descargar los buzones de correo del usuario allí el equipo realiza el chequeo. Si el servidor de correo estuviera localmente, se lograría una mejor revisión de anti-Spam, aquí también se puede crear listas negras y listas blancas.

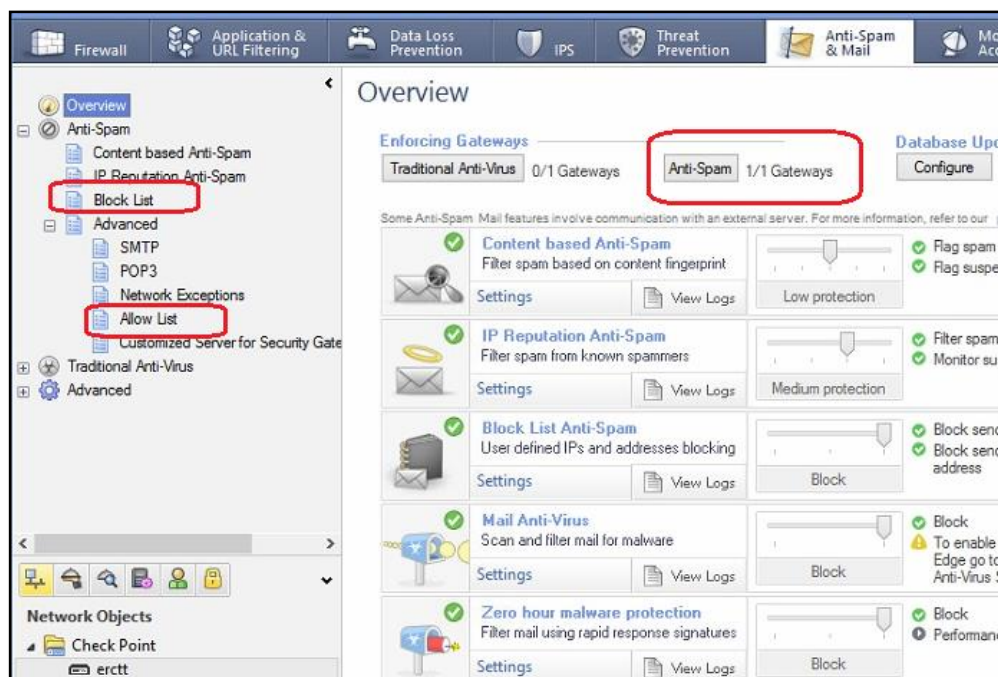


Figura 2.16 Pantalla anti-spam

## 2.8.6 IPsec VPN

En esta pestaña se encuentra la configuración de las VPN, ya sea una VPN site-to-site o client-to-site. Aquí se define la comunidad y los Gateways o grupo de usuarios participantes en la comunidad.

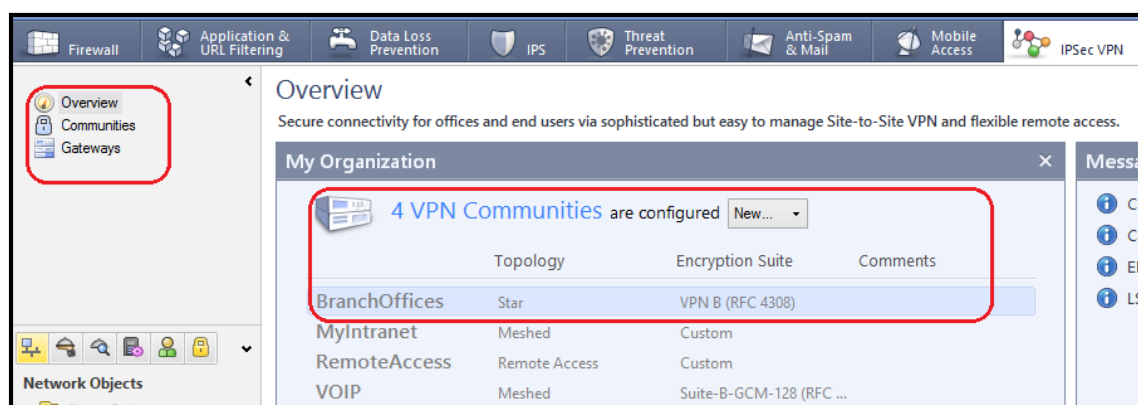


Figura 2.17 Pantalla IPSEC VPN

## 2.9 CONSOLAS DE MONITOREO EN SMARTDASHBOARD

Así también en el smartdashboard tenemos las pantallas para manejos de monitoreo: registros, eventos y reportería, actualizaciones y licenciamiento

### 2.9.1 SMARTVIEW TRACKER

Esta consola de administración es muy útil para el monitoreo de los logs de los firewalls. Adicional permite la funcionalidad de filtrar los logs ya sea por origen, destino, servicio, acción, etc...

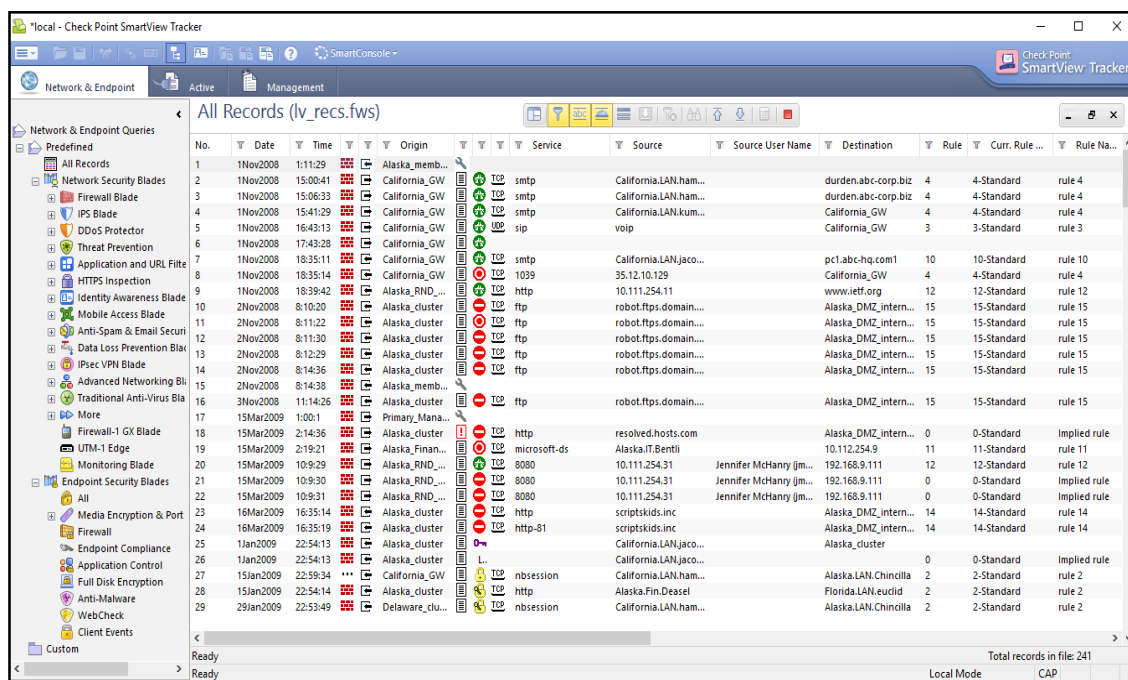
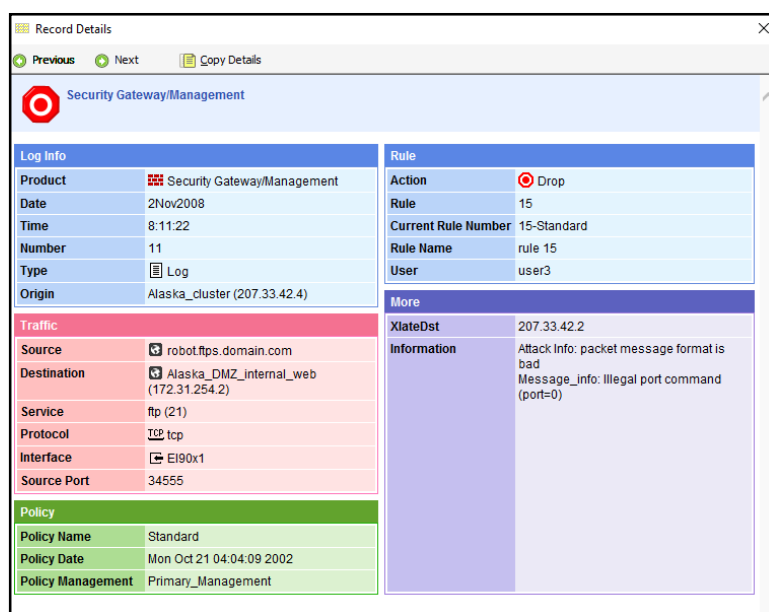


Figura 2.18 Pantalla smartview tracker

Si se desea tener mayor información sobre una línea se da doble click sobre la misma y muestra información más detallada de la misma.



The screenshot displays the 'Record Details' window for a Security Gateway/Management event. The window is divided into several sections:

- Log Info:** Product: Security Gateway/Management, Date: 2Nov2008, Time: 8:11:22, Number: 11, Type: Log, Origin: Alaska\_cluster (207.33.42.4).
- Traffic:** Source: robot.ftps.domain.com, Destination: Alaska\_DMZ\_internal\_web (172.31.254.2), Service: ftp (21), Protocol: tcp, Interface: E190x1, Source Port: 34555.
- Policy:** Policy Name: Standard, Policy Date: Mon Oct 21 04:04:09 2002, Policy Management: Primary\_Management.
- Rule:** Action: Drop, Rule: 15, Current Rule Number: 15-Standard, Rule Name: rule 15, User: user3.
- More:** XlateDst: 207.33.42.2, Information: Attack Info: packet message format is bad, Message\_Info: Illegal port command (port=0).

Figura 2.19 Pantalla smartview tracker -detalle

## 2.9.2 SMARTEVENT

Esta consola de administración sirve para tener una visión a manera de estadísticos sobre los eventos registrados de nuestra red interna hacia afuera.

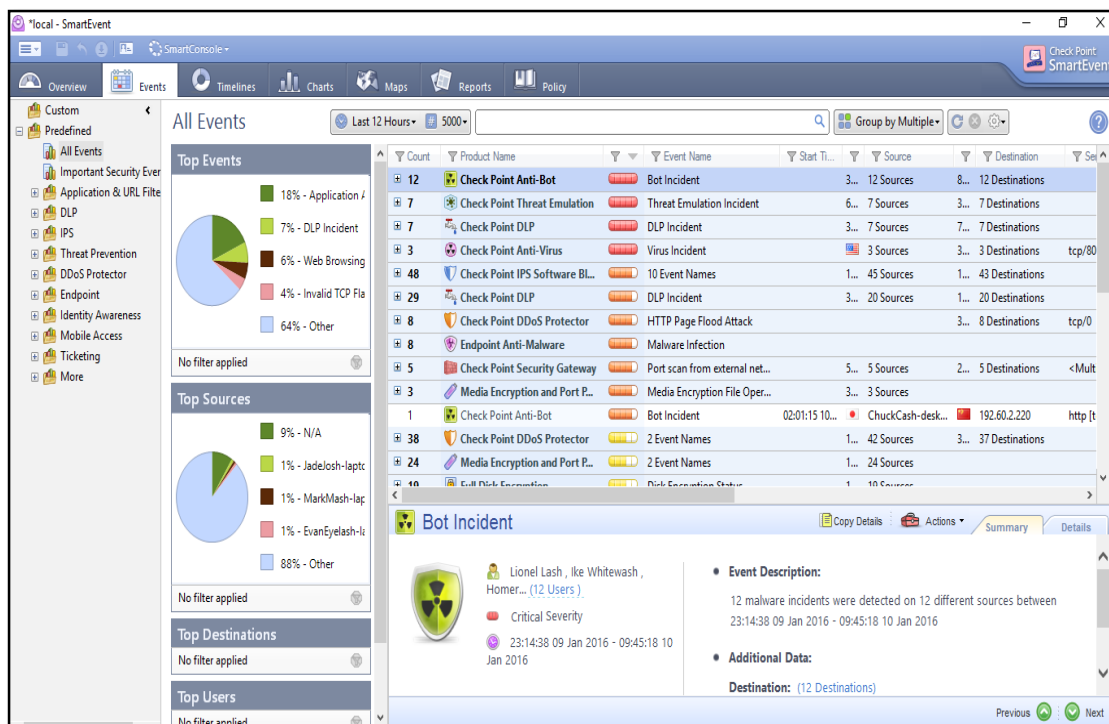


Figura 2.20 Pantalla Smartevent

### 2.9.3 SMARTUPDATE

Esta consola de administración nos permite ver las licencias y contratos activos que están en los firewalls y management. Así también adjuntar/quitar licencias DE los equipos.

Machines	IPv4 Address	IPv6 Address	Version	State	SKU	Description	Expiration D...	Has Contracts
Corporate-Cluster-1-me...	192.0.2.1		R76					
my license			NGX / R70		CP-SUITE-SAMPLE-LIC		12May2006	No
Corporate-Cluster-1-me...	192.0.2.2		R76					
my license 2			NGX / R70		CP-SUITE-SAMPLE-LIC		30Jan2006	No
Corporate-Cluster-2-me...	192.168.80.1		R76					
license 5			NGX / R70		CPMP-MEDIA-1-NGX		19Apr2006	No
Corporate-Cluster-2-me...	192.168.80.2		R76					
Corporate-DLP	10.33.124.5		R76					
Corporate-Identity-Awa...	10.34.32.5		R76					
Corporate-WAproxy-s...	172.16.2.3		R76					
eval license			NG	Requires U...			8Feb2006	No
Corporate-internal-termi...	172.16.1.10		R76					
Endpoint-1	10.14.1.132		R76					
Management	172.29.47.78		R77					
ngmt license			NG	Requires U...	CPMP-MEDIA-1-NG		11May2006	No
Management-b	172.16.1.201		R77					
Mobile_Access_London	10.74.8.73		R76					
Mobile_Access_NewY...	10.44.56.23		R76					
Remote-1-gw	198.51.100.1		R75.20					
Remote-1-web-server	192.168.2.2		R76					
Remote-2-gw	10.50.200.1		R75.20					
Remote-2-windows-do...	10.0.2.10		R76					
Remote-3-gw	10.75.25.1							
Remote-4-gw	10.125.100.1		R75.20					
Remote-5-gw	10.150.25.1		R77					
Remote_branch_gw	198.51.100.1...		R76					
VSX-gw	192.168.0.2		R76					
Vsx-Candidate-Cluster...	192.0.2.1		R75.40VS					

Figura 2.21 Pantalla SmartUpdate

## 2.9.4 SMARTREPORTER

Esta herramienta nos sirve para sacar reportes diarios, semanales, mensuales, etc., incluye reportes estándares que se pueden personalizar según las necesidades de la información que se desea conocer.



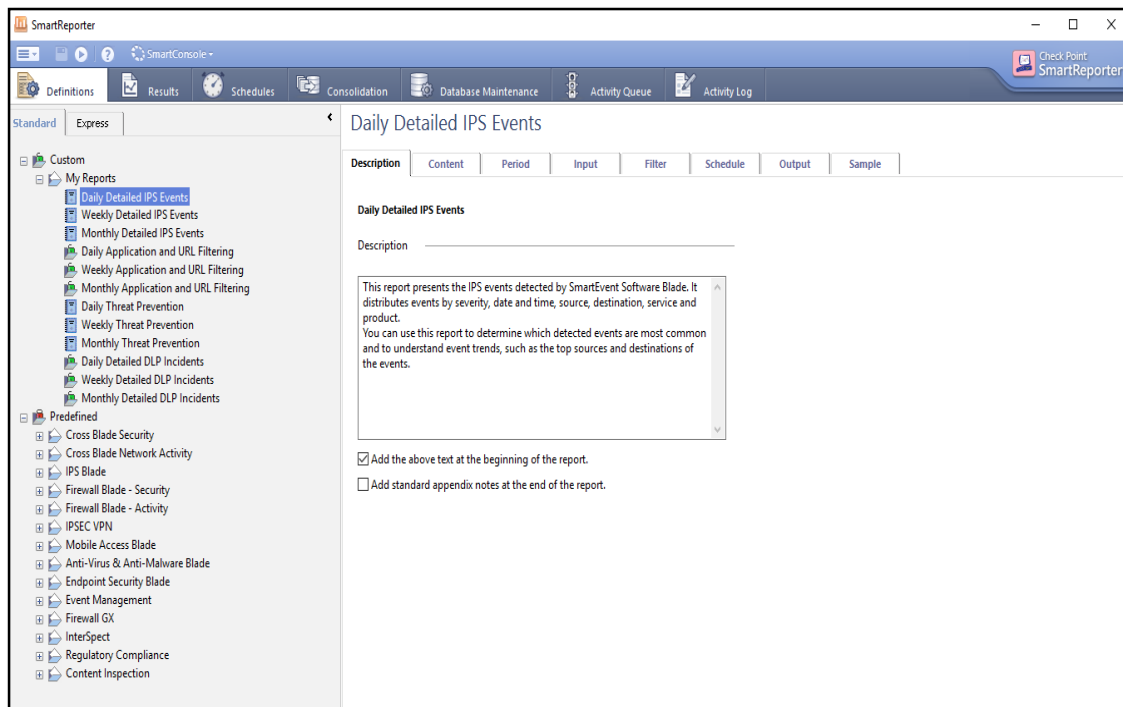


Figura 2.22 Pantalla SmartReporter

## **CAPÍTULO 3**

### **TAREAS POST IMPLEMENTACIÓN**

#### **3.1 RUTINAS DE MANTENIMIENTO**

Posterior a la implementación de la solución de seguridad perimetral, es necesario tener en cuenta ciertas rutinas de mantenimiento, las mismas ayudaran al manejo y control de los sistemas en la red en forma precisa; caso contrario sería en vano la implementación y quizás altos directivos de compañía podrían pensar que la solución no aporta a la organización.

##### **3.1.1 ENCENDIDO Y APAGADO DEL EQUIPO**

Para apagar el Security Manager/Gateway se puede usar la interfaz web o vía consola.

### 3.1.1.1 APAGADO MEDIANTE INTERFAZ WEB

Ingresamos en el navegador <https://ipaddressappliance> se nos muestra la ventana para logearse al GAIA PORTAL.

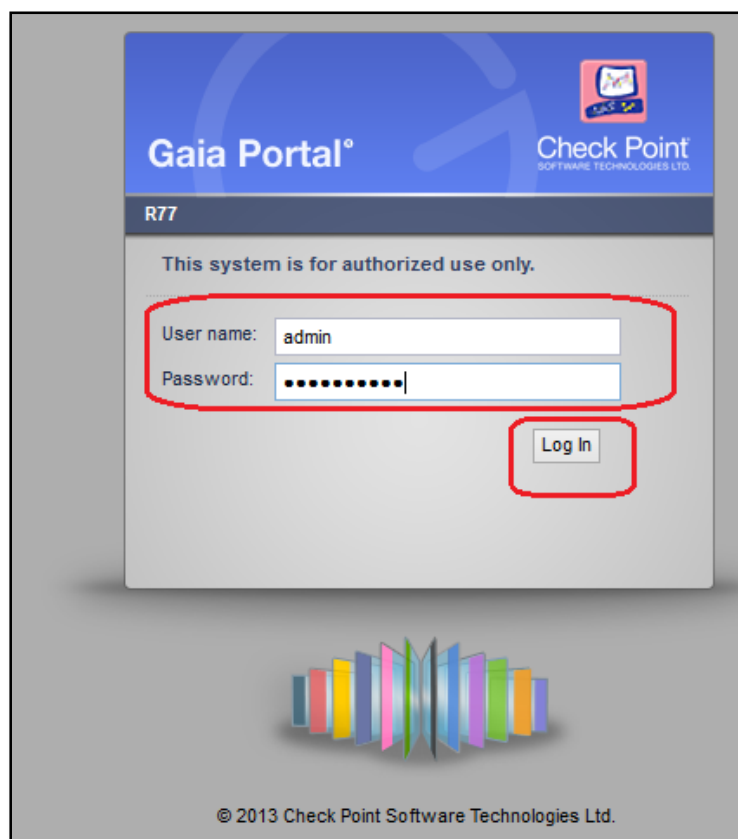


Figura 3.1 Pantalla GAIA Portal

Una vez dentro de la interfaz web del security manager/gateway, nos dirigimos al siguiente path: Maintenance → Shutdown y seleccionamos la opción Halt, como se muestra en la figura.

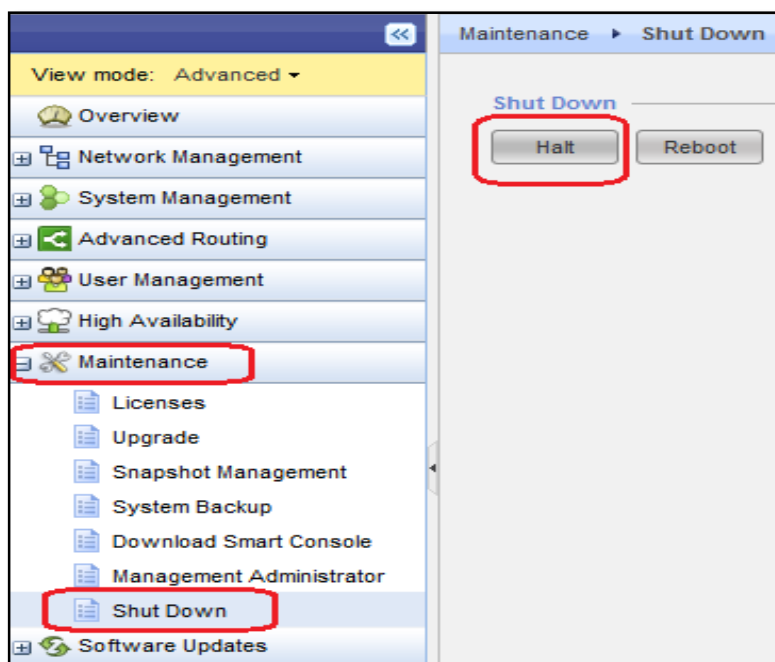


Figura 3.2 Pantalla apagado de appliance

### 3.1.1.2 APAGADO MEDIANTE CONSOLA

Si entramos por ssh al security management el comando que podemos usar para apagar el equipo depende del modo en que nos encontremos. Si estamos en modo clish, el comando es shutdown o halt, este pedirá una confirmación, a lo cual se pone “y”. Luego de eso el equipo se apaga.

```
smckp>  
smckp>  
smckp> halt  
Are you sure you want to halt?(Y/N)[N]  
—
```

Figura 3.3 Pantalla apagado por consola

Si estamos en modo expert, el comando a usar es `init 0`. Luego de eso el equipo se apaga.

```
smckp> expert
Enter expert password:

Warning! All configuration should be done through clish
You are in expert mode now.

[Expert@smckp:0]# init 0_
```

Figura 3.4 Pantalla apagado en modo experto

Es importante recalcar que para proceder al apagado del equipo se debe salir de todos los clientes SmartConsole que estén conectados al Management, es una recomendación propia de Checkpoint.

### 3.2 CREACIÓN DE RESPALDOS

Dentro del Mantenimiento del Security Manager se realiza un System Backup del Equipo, mediante la interfaz Web. En la figura siguiente se ilustra cómo realizar un System Backup.

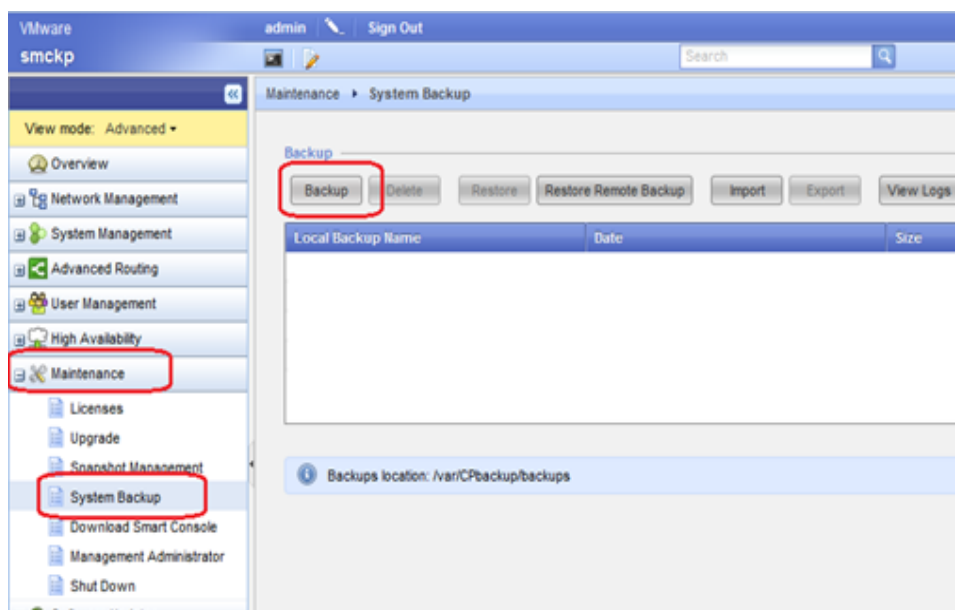


Figura 3.5 Pantalla para sacar backup

### 3.3 BORRADO DE LOGS

Borrado de logs del security Management, se lo realiza vía consola en modo expert. El path donde se encuentran almacenado los logs es: \$FWDIR/log, con el comando `ls -lh *.log` se puede verificar todos los logs los cuales están ordenados por fecha, como se puede apreciar en la figura.

```
[Expert@smckp:0]# ls -lh *.log
2013-11-01_124311_1.log  2013-12-01_204734_79.log  2013-12-02_152022_88.log  2013-12-03_084433_97.log  2013-12-03_235900.log
2013-12-01_024059_70.log  2013-12-01_221927_80.log  2013-12-02_163952_89.log  2013-12-03_102547_98.log  2013-12-04_024910_107.log
2013-12-01_063056_71.log  2013-12-01_235900.log  2013-12-02_175432_90.log  2013-12-03_121031_99.log  2013-12-04_063617_108.log
2013-12-01_091517_72.log  2013-12-02_024017_81.log  2013-12-02_191043_91.log  2013-12-03_135830_100.log  2013-12-04_091322_109.log
2013-12-01_110606_73.log  2013-12-02_061758_82.log  2013-12-02_202904_92.log  2013-12-03_153109_101.log  2013-12-04_110018_110.log
2013-12-01_124606_74.log  2013-12-02_083312_83.log  2013-12-02_215133_93.log  2013-12-03_165950_102.log  2013-12-04_123636_111.log
2013-12-01_142322_75.log  2013-12-02_095446_84.log  2013-12-02_232454_94.log  2013-12-03_183029_103.log  2013-12-04_141925_112.log
2013-12-01_160308_76.log  2013-12-02_110536_85.log  2013-12-02_235900.log  2013-12-03_200216_104.log  2013-12-04_155240_113.log
2013-12-01_173651_77.log  2013-12-02_122723_86.log  2013-12-03_023926_95.log  2013-12-03_212942_105.log  2013-12-04_171704_114.log
2013-12-01_191236_78.log  2013-12-02_135804_87.log  2013-12-03_060937_96.log  2013-12-03_230950_106.log  2013-12-04_184333_115.log
[Expert@smckp:0]#
```

Figura 3.6 Pantalla de Logs

El comando para borrar los logs es el siguiente: `rm "archivo_a_borrar".log`.

### 3.4 UPGRADE DE OS

Este Upgrade se realiza mediante la interfaz web del Gaia Portal, de la forma como se ilustra en la figura.

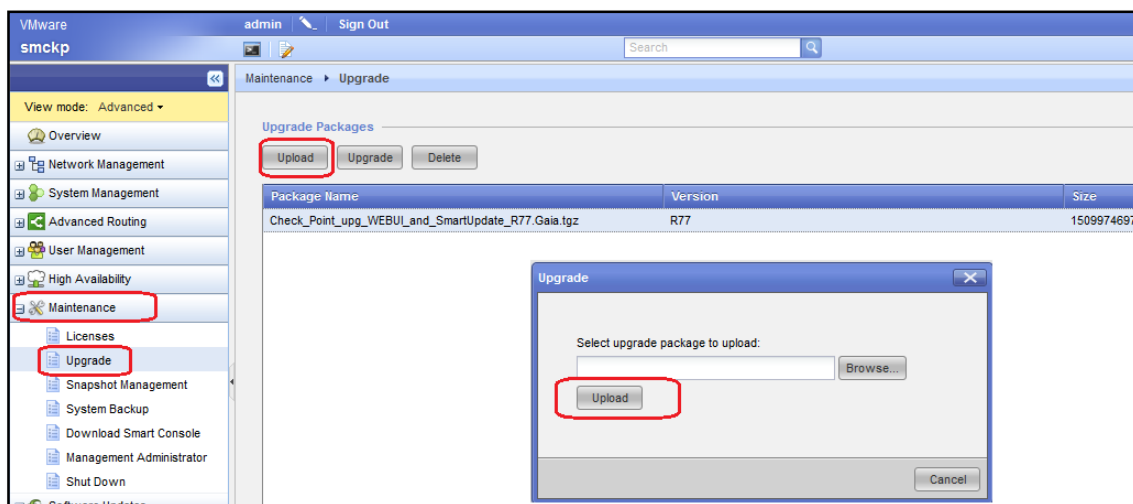


Figura 3.7 Pantalla para hacer upgrades del OS

Verificar que el archivo a subir al Security Manager/Gateway es el paquete de upgrade de la versión actual a la versión a actualizar. El proceso de upgrade solicitara realizar un snapshot antes de comenzar el upgrade para en caso de falla volver el equipo al snapshot que se realizó.

## **CAPÍTULO 4**

### **RESULTADOS**

#### **4.1 ANÁLISIS DE RESULTADOS**

Basado en los tres pilares de la seguridad informática: Disponibilidad, integridad y confidencialidad y posterior a la implementación de la solución de Seguridad Perimetral Check Point en modo standalone, en la PYME se logró lo siguiente:

##### **4.1.1 DISPONIBILIDAD**

Se logró disponibilidad de los servicios en un alto porcentaje; existe un porcentaje mínimo de no disponibilidad por mantenimientos del equipo, puesto que no existe alta disponibilidad, y por actividades internas fuera



del alcance del proyecto; mismas que pueden ser controladas. También recalcar que los colapsos de la red que anterior a la implementación de la solución perimetral sucedían fueron superados; es decir, que los ataques de denegación del servicio se bloquearon por el firewall y sus componentes.

#### **4.1.2 INTEGRIDAD**

El mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados. Fue también una de las mejoras logradas en la implementación, puesto que en el diseño se planteó red WAN, red LAN y red DMZ, de esta manera a pesar de encontrarse en la misma organización, con las políticas de seguridad se permitieron o denegaron accesos por usuario, grupos de usuarios, redes, subredes, servicios, puertos y protocolos; así también los accesos remotos por vlans.

### 4.1.3 CONFIDENCIALIDAD

La propiedad de impedir la divulgación de información a personas o sistemas no autorizados, también fue alcanzado para esto se implementó:

- Validación de accesos a servidores por usuarios permitidos en AD.
- Se registra todos los accesos a bases de datos y servidores con aplicaciones
- Existen roles por usuarios, grupos, servicios, puertos y protocolos.

De manera general, al implementar la solución de seguridad perimetral se lograron las siguientes mejoras.

- Se bloquearon todos los accesos no autorizados a la red LAN de la PYME desde el internet.
- El único frente de la organización hacia el internet es el Firewall
- Se habilitaron accesos desde el internet hacia la red PYME, utilizando VPNs.
- Se activó el control de la navegación en el internet, de manera bastante granular; por ejemplo, existía usuarios de relaciones públicas que tenían permisos para ingresar a Facebook, pero no para chatear o jugar en Facebook.

- Se restringió el acceso de los usuarios a los servidores de aplicaciones y base de datos.
- Se habilitó el IPS, Anti-bot, Anti-virus, Anti-Spam externo del firewall, de esta manera, se logró que los pc's internos sean infectados.
- La solución permitió al administrador de la red actuar de manera prolija en caso de eventualidades (ataques o falsos positivos), haciendo usos de las herramientas de monitoreo, logs, eventos y reportería.

## **CONCLUSIONES Y RECOMENDACIONES**

La implementación de la solución Check Point StandAlone logró muchas mejoras en cuanto a los tres pilares de la seguridad, entre estas tenemos.

1. La disponibilidad del servicio se superó en porcentajes muy altos, logrando que las quejas de los usuarios desaparezcan
2. La disponibilidad de los servicios pasó de no ser controladas, a poder manejarlas en tiempos o ventanas de trabajo específicas.
3. El firewall implementado logró que los ataques exteriores sean bloqueados, e incluso identificados.
4. De gran importancia fue restringir el acceso a servidores, aplicaciones o servicios el cual estaba a disponibilidad de todos, hecho que tenía muy alto riesgo puesto que la información podía ser adulterada o borrada sin lograr identificar si el usuario era interno o externo.
5. Los módulos anti-spam, anti-bot, anti-virus, IPS, permitió reducir varios ataques desde el exterior hacia los usuarios internos de la organización.

6. Se logró de manera inteligente bloquear los accesos hacia el internet, así también guardar registros de navegación y controlar el uso de ancho de banda.
7. Se permite de manera general la creación de reportes e informes sobre todos los accesos en caso de auditorías.
8. La solución de seguridad perimetral implementada, en un solo equipo, mejoró el control de las redes, accesos, y registra cada evento que ocurre internamente como en el perímetro; de esta manera se confirma porque Check Point se encuentra como líder de seguridad en el cuadrante de Gardner 2015.
9. Personalmente puedo decir, un solo equipo, instalación sencilla, costo al alcance de una PYME, y administración sencilla; es la solución más óptima para contrarrestar ataques en el perímetro, y administrar de mejor manera los usuarios internos.
10. La implementación de una solución de seguridad perimetral es bastante sencilla, solo se debe tener bien claro los lineamientos que se desea mantener en la organización. Como lo pueden haber notado, existen equipos que puede ayudarnos con nuestras necesidades y se encuentran al alcance económico de una PYME.
11. La seguridad perimetral no termina en la implementación de la misma, todo lo contrario, esta empieza cuando contamos con una solución de esta envergadura, y para esto debemos saber administrarla.

12. Finalmente, tendremos equipos como el mostrado y quizás aún muchos más robustos o con mejores características para el manejo de la seguridad en el perímetro; pero siempre existirá el factor humano; y es una brecha de seguridad que no podemos mitigar, pero si podemos controlar, y para esto se recomienda que las organizaciones también implementen políticas de seguridad informática internas.

## BIBLIOGRAFÍA

- [1]. Kirch Olaf, Dawson Terry, Guía de administración de Redes Linux, <http://es.tldp.org/Manuales-LuCAS/GARL2/garL2/x-082-2-firewall.attacks.html>, fecha de consulta enero 2016.
- [2]. Ramos Alejandro, Information Security Encyclopedia, <http://www.criptored.upm.es/intypedia/docs/es/video5/DiapositivasIntypedia005.pdf>, fecha de consulta enero 2016
- [3]. Firewalls, <http://spi1.nisu.org/recop/al01/rmoreno/definicion.html>, fecha de consulta enero 2016.
- [4]. Firewalls, <http://spi1.nisu.org/recop/al01/rmoreno/utilidades.html>, fecha de consulta enero 2016.
- [5]. Check Point, Datasheet appliance 4200  
<https://www.checkpoint.com/downloads/product-related/datasheets/4200-appliance-datasheet.pdf>
- [6]. Check Point, Gaia Installation and Upgrade guide  
[http://dl3.checkpoint.com/paid/e5/e583bb68aa9191d407d4f5e119c5647b/CP\\_R77\\_Gaia\\_Installation\\_and\\_Upgrade\\_Guide.pdf?HashKey=1452436323\\_ef\\_a1c53f9813e1f664a0cdac69585383&xtn=.pdf](http://dl3.checkpoint.com/paid/e5/e583bb68aa9191d407d4f5e119c5647b/CP_R77_Gaia_Installation_and_Upgrade_Guide.pdf?HashKey=1452436323_ef_a1c53f9813e1f664a0cdac69585383&xtn=.pdf)
- [7]. Enterprise Network Firewalls, <http://innetworktech.com/wp-content/uploads/2015/04/Magic-Quadrant-for-Enterprise-Network-Firewalls.pdf>

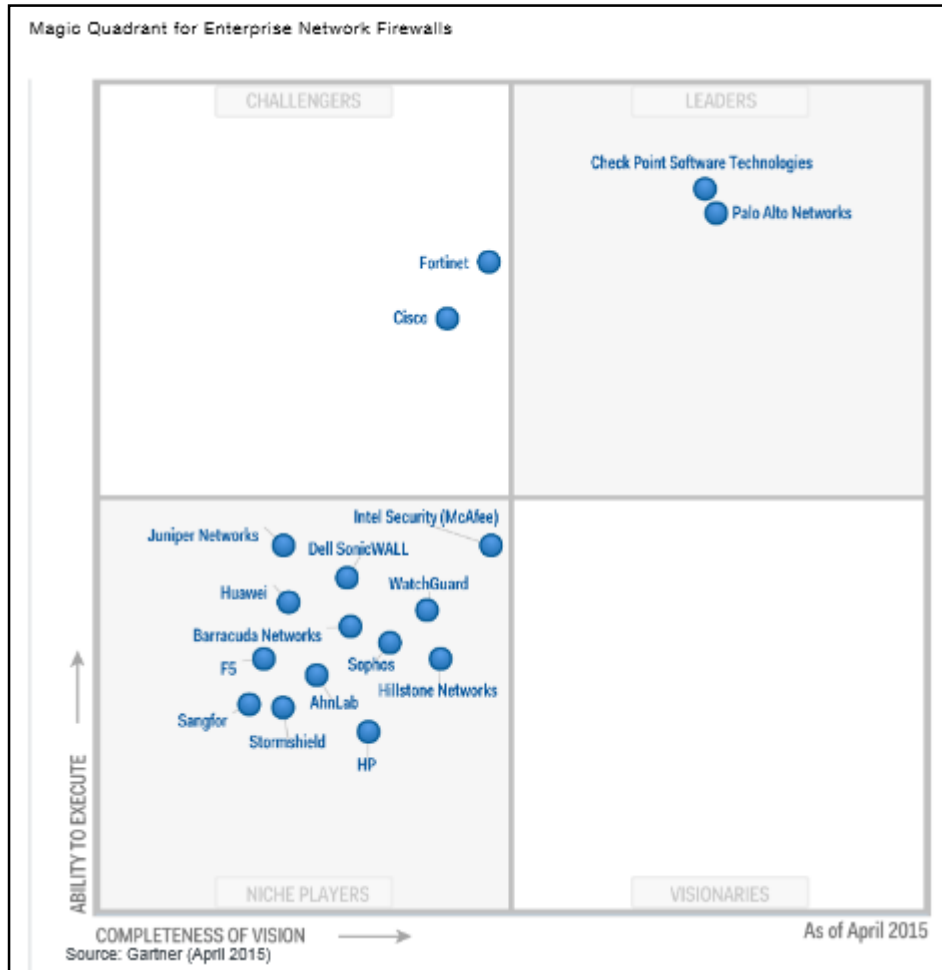
## **APÉNDICE**

### 1.- Instalación de un Firewall GAIA en modo StandAlone



## 2.- Datasheet de Check Point appliance 4200

### 3.- Cuadrante de Gartner – Líderes en Firewall [7]



4.- Ejemplo de reporte.