centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 653

Seguridad en Check Point

Julio 2023

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2023.07.26 16:13:01 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-23-120-9.
Fecha de Edición: julio de 2023.

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. INTRODUCCIÓN

El rápido crecimiento del código dañino, la creciente sofisticación de los atacantes y la aparición de nuevas amenazas de día cero requieren un enfoque diferente para mantener seguras las redes y los datos de las organizaciones. Tradicionalmente, los cortafuegos han sido el elemento fundamental en la protección del perímetro de una red, pero hoy en día no es suficiente.

Es necesario comprender y trabajar en todas las fases de la cadena de ataque para poder proteger los activos de nuestra organización. Una opción es disponer de una solución integrada. La solución de Check Point incluye funciones de seguridad como *Firewall, IPS, Anti-Bot, Antivirus,* Control de aplicaciones y Filtrado de URL para hacer frente a ciberataques y amenazas conocidas, además de la solución de emulación y extracción de amenazas, *SandBlast*, para una protección contra amenazas más sofisticadas y vulnerabilidades de día cero.

Además, es muy importante el trabajo de los administradores que se enfrentan a entornos cada vez más complejos y dinámicos. La administración de la seguridad de manera unificada simplifica la tarea de gestionar amenazas, dispositivos y usuarios al permitir vistas, detalles e informes a través de un único panel que permite a los administradores de TI gestionar fácilmente un amplio conjunto de funciones de administración de seguridad.

En esta guía se detalla cómo realizar la instalación y el mantenimiento de la solución completa de Check Point para prevenir amenazas avanzadas (NGTX: Next Generation Threat Extraction).

2. OBJETO

El objeto del presente documento es servir como guía en la instalación, configuración y mantenimiento de los cortafuegos Check Point, cubriendo todas las funcionalidades de seguridad que ofrecen.

3. ALCANCE

La información plasmada en este documento se basa en las versiones **Gaia R81 y Gaia Embedded R80.20**, sistemas operativos de los cortafuegos Check Point.

La aplicación de esta guía vendrá determinada por la correspondiente política de seguridad que corresponda (Política de Seguridad Nacional para Sistemas Clasificados, Esquema Nacional de Seguridad, etc.) y su correspondiente análisis de riesgos.

4. ACERCA DE CHECK POINT

Check Point ofrece una arquitectura de seguridad a las organizaciones desde los entornos de red hasta los dispositivos móviles.

Creada en 1993, Check Point fue pionera en el mercado de la seguridad IT con el primer firewall stateful, tecnología que sigue siendo la base para algunas de las tecnologías actuales.

La compañía actualmente mantiene 70 patentes estadounidenses y más de 60 patentes pendientes.

En cuanto a reconocimiento del mercado, Check Point es reconocido por algunos analistas y tests independientes:

- *Firewall* con mayor efectividad de seguridad en Miercom Next-Gen Firewall Security Efficacy Report 2023.
- Nivel AAA (máximo) en CyberRatings Enterprise Firewalls 2021 Test.
- Líder en The Forrester Wave™: Enterprise Firewalls, 2022.
- Líder en Gartner's "Enterprise Network Firewall Magic Quadrant" (1999-2002, 2004-2022).
- *Líder en Gartner's "Mobile Data Protection Magic Quadrant"* (2001-2015).
- *Líder en Gartner's "Unified Threat Management (UTM) Magic Quadrant"* (2010-2018).
- *Market share leader in worldwide combined Firewall and UTM appliance revenue (IDC*
- *FY 2015 Security Appliance Tracker).*
- NSS Labs "*Recommend*" para Breach Detection Systems (BDS) (NSS Labs 2015-2016).
- NSS Labs "*Recommend*" para Next Generation Firewall (NSS Labs 2011 – 2016).
- NSS Labs "*Recommend*" para Network Firewall (NSS Labs 2011, 2013).
- NSS Labs "*Recommend*" para IPS (NSS Labs 2011 – 2013).
- A destacar el reciente reconocimiento de NSS Labs en su *"Breach Prevention Systems (BPS)"* test en el que Check Point Sandblast ha sido la tecnología con mejor resultado en cuanto a prevención de amenazas y con el mejor TCO.

5. AMENAZAS ACTUALES

La rápida transformación digital de las organizaciones implica cada vez mayores exigencias de seguridad. Las organizaciones convergen aplicaciones y datos en redes IP. Los equipos de sobremesa están siendo progresivamente reemplazados por portátiles, tabletas y dispositivos propios de los empleados (BYOD), en tanto que las aplicaciones se van moviendo desde *el data center* hacia nubes híbridas, alimentadas por dispositivos IoT o externalizadas completamente bajo modelos de software como servicio (SaaS). Además, regulaciones como GDPR han generado nuevos requisitos de control de datos a implementar en estos entornos.

La cantidad y tipología de las amenazas se están acelerando. La amplia superficie de ataque de los entornos de nube híbrida, la movilidad y las redes de IoT suponen un mayor número de nuevos puntos de ataque para ser explotados. Mientras tanto, las organizaciones criminales o actores a nivel de estado han generado una tecnología de ciberataque más potente, disponible para unos adversarios cada vez en mayor número y bien organizados.

Prácticamente todas las organizaciones TIC buscan mejorar su capacidad para mitigar riesgos con un nivel de inversión razonable y sostenible. Pero hay tres retos que lo hacen extremadamente difícil:

- Un panorama de amenazas en continuo cambio.
- La enorme cantidad y diversidad de datos, aplicaciones e infraestructuras de la organización que deben ser protegidos (datos móviles, entornos cloud/SaaS, outsourcing de terceros…).
- Personal de seguridad que pueda desarrollar estrategias técnicas efectivas y sostenibles en el tiempo.

El despliegue de productos de prevención tradicionales ha dado como resultado una gran cantidad de datos de registro y alertas, la mayoría de los cuales han sido ignorados. Este enfoque ha traído más complejidad, con múltiples productos y sistemas de gestión independientes, que no comparten inteligencia de políticas y amenazas, y que pueden tener carencias defensivas. En definitiva, infraestructuras de seguridad más complejas y costosas, pero que no mejoran la protección.

La aproximación de Check Point ante estos desafíos es *Check Point Infinity*, que combina una tecnología de prevención, una política de seguridad unificada y un modelo operacional cuya implementación incluye redes, entornos de nube y dispositivos móviles.

Infinity se divide en tres partes:

- **Prevención de amenazas**: capacidades de protección desplegadas a través de redes, entornos de nube y dispositivos móviles combinando una solución de prevención de amenazas multicapa.
- **Plataforma de inteligencia de amenazas**: Check Point Threat Cloud aglutina y distribuye inteligencia de amenazas y actualizaciones de protección en tiempo real.
- **Gestión de amenazas**: interfaz de gestión unificada que permite utilizar políticas de riesgos orientadas al negocio y convertirlas en protecciones de seguridad, con API para proyectos de integración con otras aplicaciones e infraestructuras de TI.

6. ARQUITECTURA CHECK POINT

La arquitectura de gestión de seguridad de Check Point es una arquitectura orientada a objetos que utiliza representaciones gráficas de entidades del mundo real, como usuarios y puertas de enlace. Estas entidades se configuran, administran y supervisan a través de una única consola de administración. Hay tres componentes esenciales de la arquitectura de gestión de seguridad de Check Point: SmartConsole, Security Management Server y Security Gateway/Quantum Spark.

- **SmartConsole:** Es una interfaz gráfica de usuario (GUI) que se utiliza para administrar los objetos que representan elementos de red, servidores y *Security Gateways/Quantum Spark*. Estos objetos se utilizan en *SmartConsole* para muchas tareas, incluida la creación de Políticas de seguridad. También se usa para monitorizar el tráfico a través de registros y administrar *Software Blades*, licencias y actualizaciones.
- **Security Management Server**: Cuando se crea una política de seguridad en *SmartConsole*, se almacena en el servidor de gestión de seguridad. El *Security Management Server* luego distribuye esa Política de Seguridad a los diversos *Security Gateways/Quantum Spark*. También se usa para mantener y almacenar las bases de

datos de una organización, incluidas las definiciones de objeto y los archivos de registro para todos los *Security Gateways*.

- **Security Gateway/Quantum Spark**: Una puerta de enlace en la que está habilitada el *Software Blade* de *Firewall*. También se conoce como la propia máquina que hace de cortafuegos. Las pasarelas de seguridad se implementan en los puntos de acceso a la red o en los puntos donde la red de la organización está expuesta al tráfico externo o interno. Protegen la red utilizando la Política de Seguridad que le envía el *Security Management Server*. Los dispositivos Security Gateway y Quantum Spark no se diferencian a nivel de funcionalidades de seguridad proporcionadas. Su principal cambio es el sistema operativo utilizado internamente.

Controlar el tráfico de red ayuda a mejorar en general el rendimiento de la red y la seguridad organizacional. El cortafuegos denegará o permitirá el tráfico basándose en reglas definidas en la Política de seguridad. Las siguientes tecnologías son las implicadas en denegar o permitir tráfico:

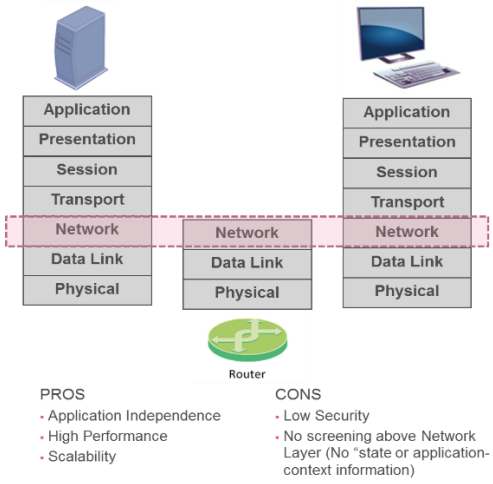
- *Packet Filtering.*
- *Stateful Inspection.*
- *Application Layer Firewall.*

6.1 PACKET FILTERING

Los mensajes se dividen en paquetes que incluyen los siguientes elementos:

- Dirección de origen.
- Dirección de destino.
- Puerto origen.
- Puerto destino.
- Protocolo.

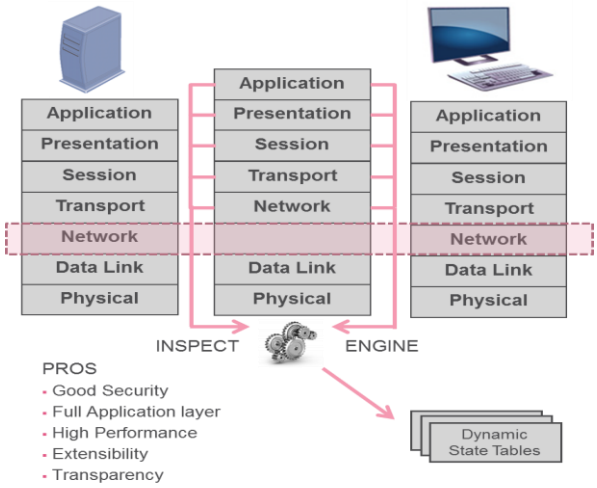
Packet Filtering es la forma más básica de un cortafuegos. Su primer propósito es controlar el acceso a segmentos de red específicos según lo definido por un conjunto de reglas de seguridad. *Packet Filtering* funciona sobre la capa de red y de transporte de la arquitectura de red. Los paquetes son individualmente enviados a su destino por varias rutas. Una vez los paquetes llegan a su destino se recompilan para construir el mensaje original.



6.2 STATEFUL INSPECTION

Stateful Inspection analiza las direcciones de origen y destino del paquete, los puertos de origen y destino, el protocolo y el contenido. Con esta funcionalidad el estado de conexión es monitorizado y las tablas de estado son creadas para compilar la información. Las tablas de estado contienen información útil con respecto a la monitorización del rendimiento a través de un *Security Gateway/Quantum Spark*. Como resultado, el filtrado incluye contenido que ha sido establecido por los paquetes anteriores que han pasado a través del cortafuegos.

Por ejemplo, *Stateful Inspection* proporciona una medida de seguridad contra el escaneo de puertos cerrando todos los puertos hasta que se solicite el puerto específico.



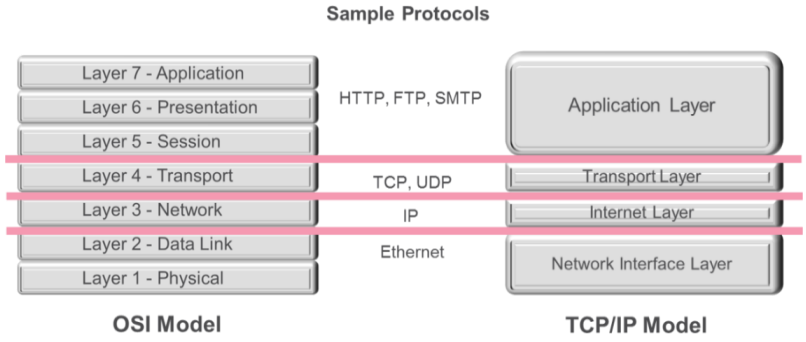
El motor *INSPECT* de Check Point, que está instalado en el *Security Gateway/Quantum Spark*, se usa para extraer información relacionada con el estado de los paquetes y almacenar esa información en las tablas de estado. Las tablas de estado son componentes clave de la tecnología *Stateful Inspection* porque son vitales para mantener la información del estado necesaria para inspeccionar correctamente los paquetes. Cuando llegan nuevos paquetes, sus contenidos se comparan con las tablas de estado para determinar si son negados o permitidos.

Stateful Inspection difiere del filtrado de paquetes en que examina en profundidad un paquete no solo en su encabezado, sino también en el contenido del paquete a través de la capa de

aplicación para determinar más sobre el paquete que solo información sobre su origen y destino. Además, el filtrado de paquetes requiere crear dos reglas para cada usuario que necesita acceder a los recursos, se necesita una regla de solicitud saliente y se requiere una segunda regla para la respuesta entrante para la misma conexión. La creación de *Stateful Inspection* eliminó la necesidad de dos reglas. El cortafuegos recuerda cada respuesta para una solicitud existente utilizando las tablas de estado. Por lo tanto, solo se requiere una regla para cada conexión.

6.3 APLICATION LAYER FIREWALL

Muchos ataques tienen como objetivo explotar una red a través de las aplicaciones de red, en lugar de atacar directamente al cortafuegos. Los cortafuegos de capa de aplicación operan en dicha capa de la pila de protocolos TCP/IP para detectar y prevenir ataques contra aplicaciones y servicios específicos. Proporcionan filtrado, exploración antivirus y control de acceso para aplicaciones de red, como correo electrónico, FTP y HTTP. Estos cortafuegos pueden tener servidores proxy o software de aplicación especializado agregado.



Los cortafuegos de capa de aplicación inspeccionan el tráfico a través de las capas inferiores del modelo TCP/IP incluyendo la capa de aplicación. Dado que los *Application Layer Firewalls* son conscientes de las aplicaciones, pueden examinar sesiones individuales y decidir descartar un paquete según la información del protocolo de la aplicación. Los cortafuegos de aplicación inspeccionan el contenido del tráfico y aplican reglas de acceso permitiendo o bloqueando por sesión o conexión en lugar de filtrar conexiones por puerto, como el filtrado de paquetes.

Los paquetes se inspeccionan para garantizar la validez del contenido y evitar *exploits* incrustados en el contenido. El alcance del filtrado se basa en las reglas definidas en la política de seguridad de red.

6.4 SECURE INTERNAL COMMUNICATION

Secure Internal Communication (SIC) es un medio por el cual las plataformas y los productos se autentican entre sí. Crean conexiones confiables entre puertas de enlace, servidores de administración y otros componentes de Check Point. La comunicación interna segura es necesaria para la instalación de políticas en las puertas de enlace y para enviar logs entre las puertas de enlace y los servidores de administración. Una vez que se establece SIC, el servidor de administración y sus componentes se identifican por sus nombres en lugar de la dirección IP. Hay tres métodos de autenticación:

- Certificados.
- SSL basado en estándares para la creación de canales seguros.
- 3DES o AES128 para encriptación.

6.4.1 INTERNAL CERTIFICATE AUTHORITY

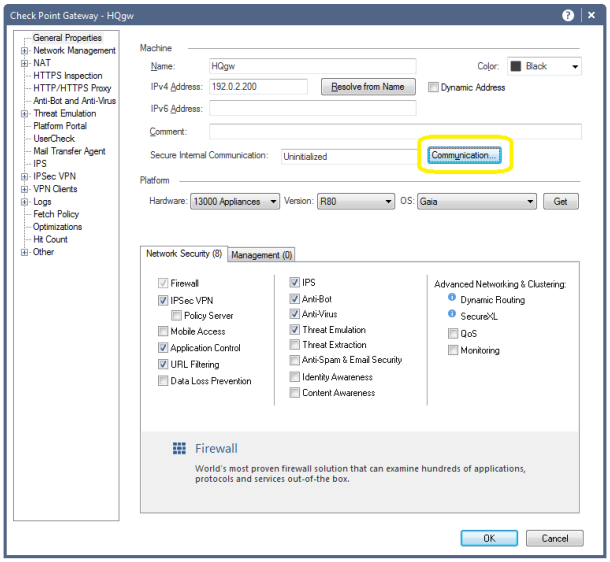
La Autoridad de Certificación Interna (ICA) se crea durante el proceso de instalación principal del servidor de administración de seguridad. Es responsable de emitir los siguientes certificados para autenticarse:

- SIC: Autentica entre puertas de enlace o entre puertas de enlace y servidores de administración de seguridad.
- Certificados VPN: Autentica entre los miembros de la comunidad VPN para crear el túnel VPN.
- Usuarios: Autentica el acceso del usuario según la autorización y los permisos.

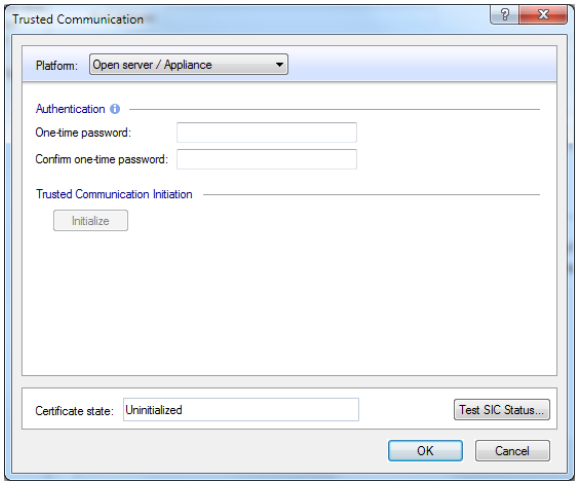
Una puerta de enlace y un servidor de administración usan una contraseña de un solo uso para establecer inicialmente la confianza. La ICA firma y emite un certificado a la puerta de enlace. La puerta de enlace y el servidor de administración se autenticarán a través de SSL utilizando una contraseña de un solo uso. El certificado se descarga y se almacena en la puerta de enlace y se establece la confianza. Ahora, la puerta de enlace puede comunicarse de manera segura con otras puertas de enlace de Check Point y servidores de administración que tienen un certificado de seguridad firmado por la misma ICA.

Para inicializar la confianza:

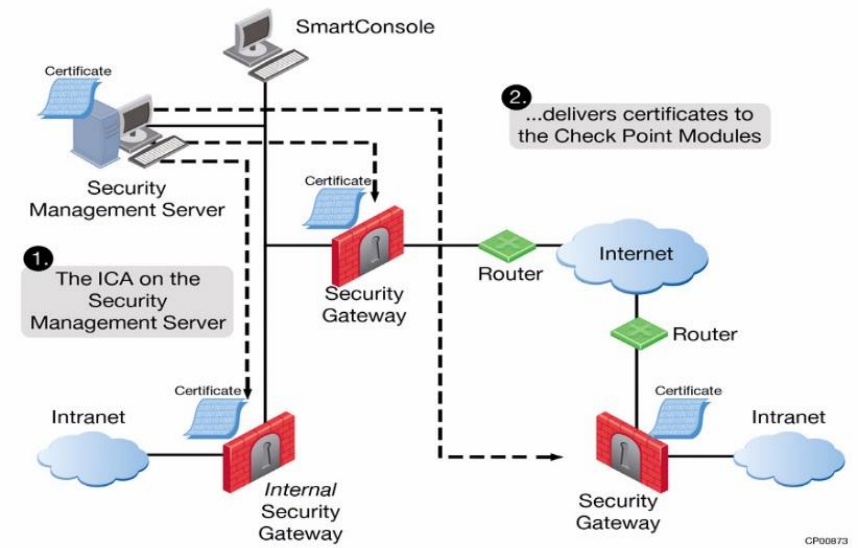
- En *SmartConsole*, ir a la página “General Properties” del objeto de la puerta de enlace.
- En la sección “Machine”, pulse en el botón “Comunication”.



- En la sección “*Autentication*”, ingresar y confirmer la contraseña de un solo uso. Esta contraseña de un solo uso debe estar tanto en la puerta de enlace como en el servidor de administración.



- En la sección "*Trusted Communication Initialization*", pulsar en "*Initialize*".
- Publicar los cambios.



Si el estado de confianza se ha visto comprometido (se han filtrado claves o perdido certificados) es posible restablecerlo. Una vez que se ha establecido SIC, debe restablecerse tanto en *Security Management Server* como en *Security Gateway/Quantum Spark*.

Al restablecer el SIC, *Security Management Server* revoca el certificado de *Security Gateway/Quantum Spark* y almacena la información del certificado en la Lista de revocación de certificados (CRL).

Una vez que se restablece el estado de confianza, se actualiza con el número de serie del certificado revocado. El ICA firma la CRL actualizada y la emite a todas las puertas de enlace durante la siguiente conexión SIC. Si dos puertas de enlace tienen diferentes CRL, no pueden autenticarse.

Para restablecer el estado de confianza:

- En *SmartConsole*, "*General Properties*" del objeto de la puerta de enlace.
- En la sección "Machine", pulse en el botón "Comunication".

- En la parte inferior, al lado del estado del certificado, pulse en “Restablecer”.
- Publique los cambios.
- Instalar la política en las puertas de enlace para implementar la CRL actualizada en todas las puertas de enlace.

El estado de confianza también debe restablecerse en la puerta de enlace. Para establecer un nuevo estado de confianza para una puerta de enlace:

- Abra la interfaz de línea de comandos (CLI) en la puerta de enlace.
- Ejecute el siguiente comando: *cpconfig*
- Escriba el número de la opción SIC, presione “Enter” y confirme.
- Ingrese y confirme la clave de activación.
- Cuando termine, ingrese el número para Salir.
- Espere a que los procesos se detengan y reinicien automáticamente.
- En *SmartConsole*, navegue a “Propiedades generales” del objeto de la puerta de enlace.
- Complete los pasos requeridos para inicializar la confianza.

6.5 TOPOLOGÍA DE RED

Hay que tener en cuenta la red existente en el momento de la implementación, ya que puede requerir la reconfiguración del esquema de enrutamiento. Hay tres opciones de implementación disponibles: *Standalone*, *Distribuido* y *Modo Bridge*.

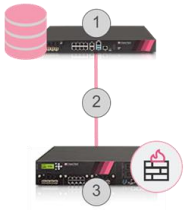
6.5.1 STANDALONE

En una implementación Standalone, el Security Management Server y el Security Gateway se instalan en el mismo dispositivo. Esta topología no se encuentra disponible en los dispositivos Quantum Spark al no ser posible desplegar en estos dispositivos el Security Management Server component.

Item	Description
1	Security Management Server component
2	Standalone server
3	Security Gateway component

6.5.2 DISTRIBUIDO

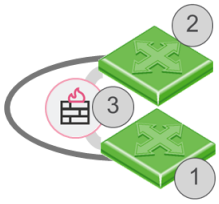
En un entorno distribuido, el *Security Gateway/Quantum Spark* y el *Security Management Server* están instalados en diferentes dispositivos.



Item	Description
1	Security Management Server
2	Network connection
3	Security Gateway

6.5.3 MODO BRIDGE

La implementación del *Modo Bridge* se trata de agregar un *Security Gateway/Quantum Spark* a un entorno existente sin cambiar el enrutamiento.



Item	Description
1	Switch
2	Switch
3	Security Gateway Firewall bridging Layer-2 traffic over the one IP address, with a subnet on each side using the same address.

6.6 VIRTUAL SYSTEM (VSX)

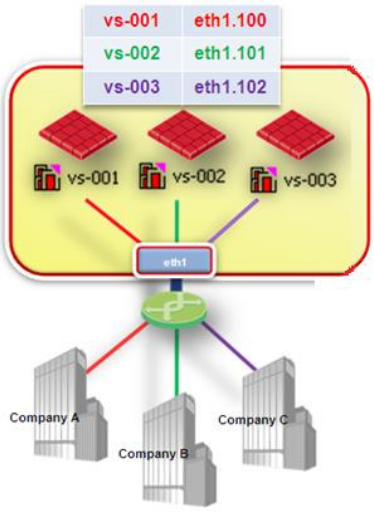
VSX (Virtual System Extension) es una solución VPN y de seguridad para entornos a gran escala basada en *Security Gateway/Quantum Spark*. VSX permite proteger redes múltiples o VLAN frente a recursos compartidos, como Internet y/o DMZ, siendo compatible con los servicios IPS.

VSX incorpora la misma tecnología *Stateful Inspection* y *Software Blades* utilizada en Check Point. Se administra utilizando un Servidor de administración de seguridad o un Servidor multidominio, como una arquitectura de administración unificada.

VSX contiene un conjunto de dispositivos virtuales que funcionan como componentes físicos de red, como *Security Gateway/Quantum Spark*, enrutadores, conmutadores, interfaces e incluso cables de red. VSX permite implementar una funcionalidad de cortafuegos y VPN reduciendo la inversión en hardware.

Cada sistema virtual funciona como un Security Gateway*/Quantum Spark*, que generalmente protege una red específica. Cuando los paquetes llegan al VSX Gateway, se envía tráfico al sistema virtual que protege la red de destino. El sistema virtual inspecciona todo el tráfico y lo permite o rechaza según las reglas definidas en la política de seguridad.

Para comprender mejor cómo funcionan las redes virtuales, es importante comparar los entornos físicos de red con sus contrapartes virtuales (VSX). Si bien las redes físicas constan de muchos componentes de hardware, las redes virtuales VSX residen en una única pasarela VSX configurable, o clúster, que define y protege múltiples redes independientes, junto con sus componentes virtuales.



Un *Gateway VSX* es una máquina física que aloja dispositivos virtuales, con la funcionalidad de sus contrapartes de red física, tales como: *Security Gateways/Quantum Sparks*, enrutadores y conmutadores.

Un *Gateway VSX* realiza las siguientes tareas:

- Se comunica con el servidor de administración para implementar, configurar y administrar todos los dispositivos virtuales.
- Administra la sincronización de estado para alta disponibilidad y para compartir la carga en el clúster.

Un sistema virtual es un dominio de enrutamiento y seguridad que proporciona la funcionalidad de un *Security Gateway/Quantum Spark*. Varios sistemas virtuales se pueden ejecutar simultáneamente en un único *Gateway VSX*.

Cada sistema virtual funciona de forma independiente manteniendo sus propios módulos de software, interfaces, direcciones IP, tabla de enrutamiento, tabla ARP y configuración de enrutamiento dinámico. Cada sistema virtual también mantiene los siguientes elementos propios:

- Tablas de estado: Cada sistema virtual tiene sus propias tablas de kernel con configuración y datos de tiempo de ejecución, como conexiones activas e información de túneles IPSec.
- Políticas de seguridad y VPN: Cada sistema virtual impone su propia seguridad y las políticas de VPN. Las políticas se recuperan del servidor de gestión y se almacenan por separado en el disco local y en el kernel. En un entorno de administración de seguridad multidominio, cada base de datos de dominio se mantiene por separado en el servidor de administración y en la puerta de enlace VSX.
- Parámetros de configuración: Cada sistema virtual mantiene su propia configuración, como la configuración de IPS. Diferentes sistemas virtuales pueden ejecutarse en modo capa 2 o capa 3 y coexistir en la misma puerta de enlace VSX.
- Configuración de registro: Cada sistema virtual mantiene sus propios registros y ejecuta el registro de acuerdo con sus propias reglas y configuración.

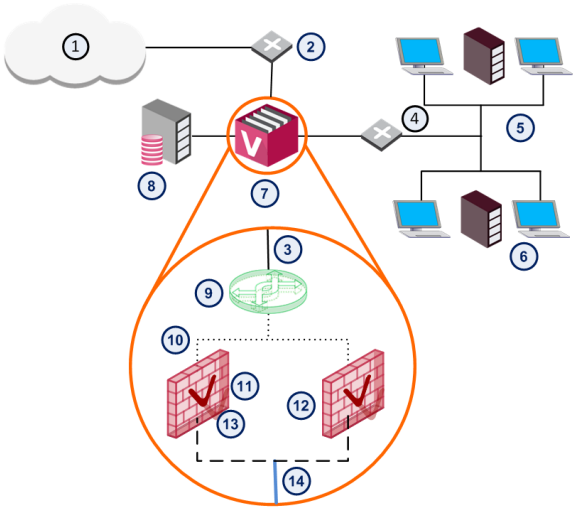
Un *virtual router* es un dominio de enrutamiento independiente dentro de un *Gateway VSX*, que realiza la funcionalidad de los enrutadores físicos. Los enrutadores virtuales son útiles para conectar múltiples sistemas virtuales a una interfaz compartida y para enrutar el tráfico de un sistema virtual a otro. Los enrutadores virtuales admiten enrutamiento dinámico.

Los enrutadores virtuales realizan funciones de enrutamiento con el siguiente tráfico:

- Los paquetes que llegan a la puerta de enlace VSX a través de una interfaz compartida para el sistema virtual designado en función de la dirección IP de origen o de destino.
- Tráfico procedente de sistemas virtuales dirigido a una interfaz compartida o a otros sistemas virtuales.
- Tráfico hacia y desde recursos compartidos de la red, como una DMZ.

Al igual que con los enrutadores físicos, cada enrutador virtual mantiene una tabla de enrutamiento con una lista de entradas de ruta que describen las redes conocidas y las instrucciones sobre cómo llegar a ellas. Según los requisitos de implementación, se pueden configurar múltiples enrutadores virtuales.

También existen los conmutadores virtuales que proporcionan conectividad de capa 2, conectando los sistemas virtuales y facilitando compartir una interfaz física común sin segmentar la red IP existente. Al igual que con un conmutador físico, cada conmutador virtual mantiene una tabla de reenvío con una lista de direcciones MAC y sus puertos asociados.



Item	Description
1	Internet
2	Router
3	Physical interface
4	VLAN Switch
5	Network 1
6	Network 2
7	VSX Gateway

Item	Description
8	Security Management Server
9	Virtual Switch
10	Warp interface
11	Virtual System 1
12	Virtual System 2
13	VLAN Interface
14	VLAN Trunk

Notas:

- *Warp Links* conectan el conmutador virtual a cada sistema virtual.
- Una interfaz física conecta el conmutador virtual a un enrutador externo.
- Las interfaces de VLAN conectan los sistemas virtuales al conmutador de VLAN, a través de una troncal de VLAN.
- El VLAN switch se conecta a las redes protegidas.

Se puede configurar un sistema de seguridad para ejecutar *fwk* como un proceso de 64 bits. Esto permite que *VSX Virtual Systems* use más de 4 GB de RAM, lo que aumenta significativamente la capacidad de conexiones simultáneas para cada sistema virtual.

Utilizar el comando *vs_bits* para configurar *fwk* para que se ejecute en el modo de 64 o 32 bits. El sistema se reinicia automáticamente cuando ejecuta el comando.

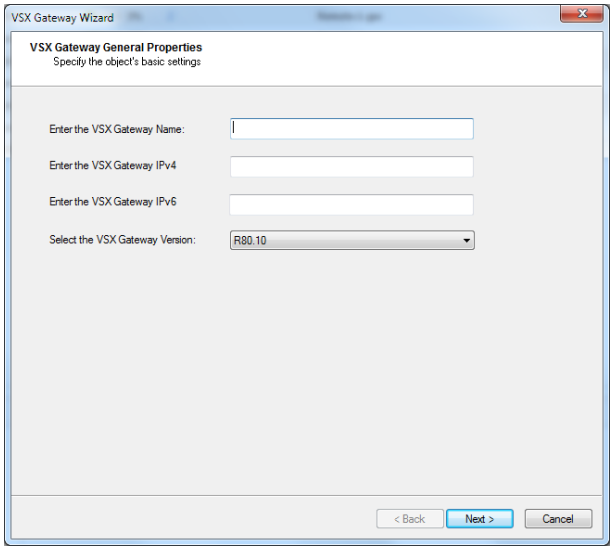
Importante: ejecute el comando *vs_bits* solo desde un contexto *VS0.*

```
vs_bits [-stat | 32 | 64 ]
```

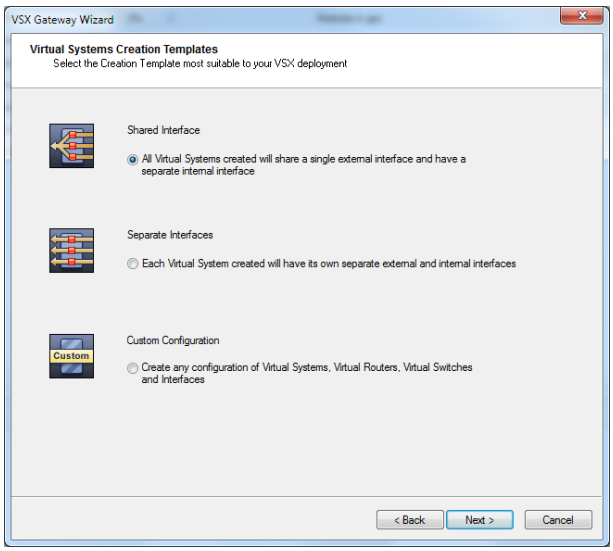
Parameter	Description
`stat`	Shows the current `fwk` mode
`32`	Run `fwk` in the 32 bit mode
`64`	Run `fwk` in the 64 bit mode

Nota: El *Gateway VSX* ejecutará automáticamente *cpstop*; *cpstart*

Para crear un *Gateway VSX* ir a *Nuevo Network Object* ➔ *Gateways and servers* ➔ *VSX* ➔ *Gateway*

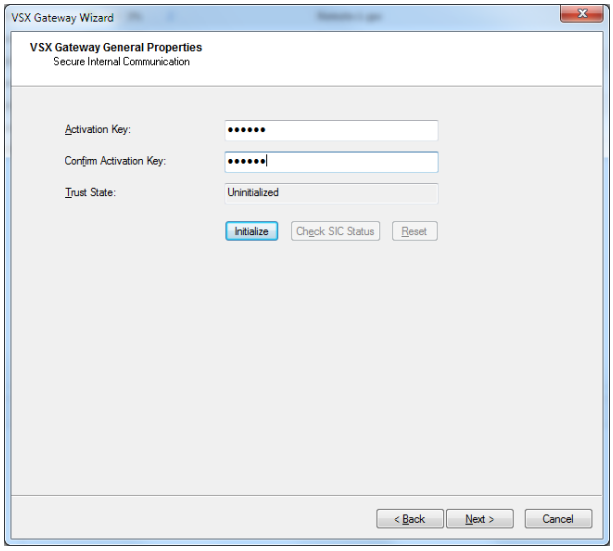


Tras fijar el nombre y la dirección IP, es necesario seleccionar el modo de funcionamiento según distintas "*templates*" o de forma "*customizada*":



- *Shared Interface*: Todo los Virtual System creados comparten una interfaz externa e interfaces separadas en el lado interno.
- *Separate Interfaces*: Cada Virtual System tiene su propia interfaz externa e interna.
- *Custom Configuration*: Crea una configuración con Virtual Routers, Virtual *Switches* e interfaces.

Y además establecer el SIC.


VSX Gateway Wizard
VSX Gateway General Properties
Secure Internal Communication
Activation Key:
Confirm Activation Key:
Trust State:
Uninitialized
Initialize
Check SIC Status
Reset
< Back
Next >
Cancel

7. CONFIGURACIÓN BÁSICA

En este apartado se tratarán los conceptos básicos de configuración a la hora de desplegar el dispositivo.

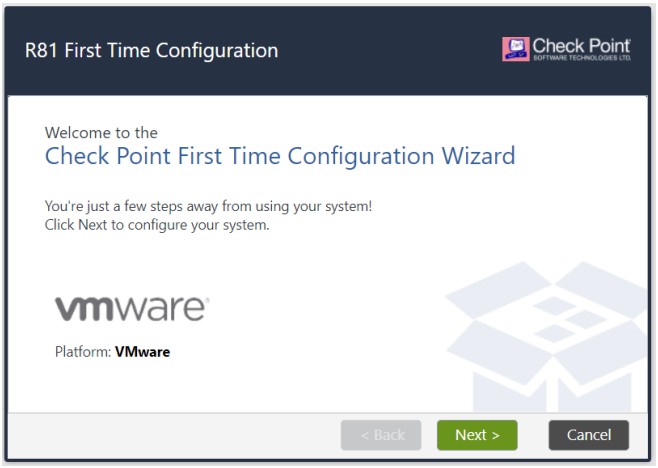
7.1 WIZARD INICIAL

En función del tipo de dispositivo (Security Gateway o Quantum Spark) el asistente de configuración inicial variará.

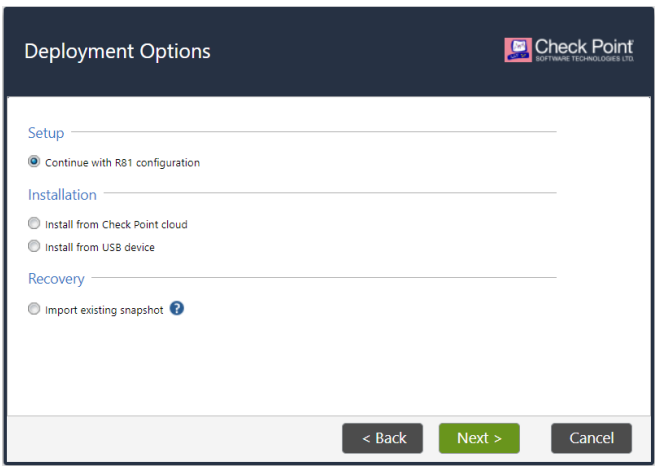
7.1.1 SECURITY GATEWAY

Iniciamos un navegador de Internet, como Firefox o Internet Explorer.

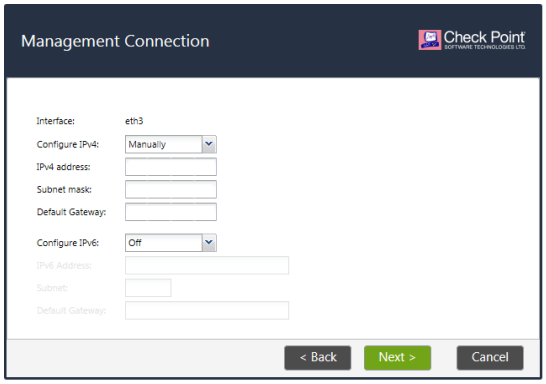
- En el campo de dirección escriba lo siguiente: https://192.168.1.1
- Presionar "Entrar" y el navegador debe advertir que el Certificado de seguridad del sitio no es de confianza.
- Ignorar esta advertencia y continuar con la pantalla de inicio de sesión.
- Iniciar sesión con nuestras credenciales (por defecto admin/admin) y mostrará la siguiente pantalla:



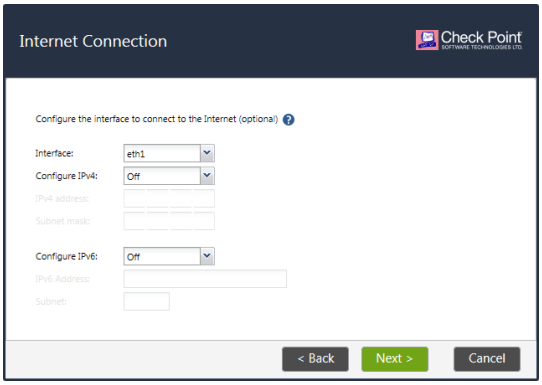
- Pulsar en "Next", y el sistema mostrará una página con las siguientes opciones de despliegue:



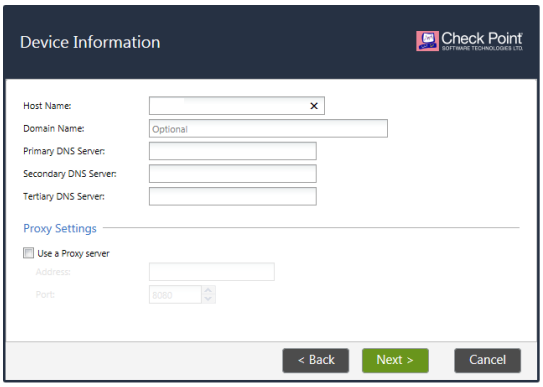
- Verificar que la siguiente opción esté seleccionada: *"Continue with Gaia R.81 configuration"*.
- Pulsar en "Next" y el sistema mostrará la página de "Management Connection":



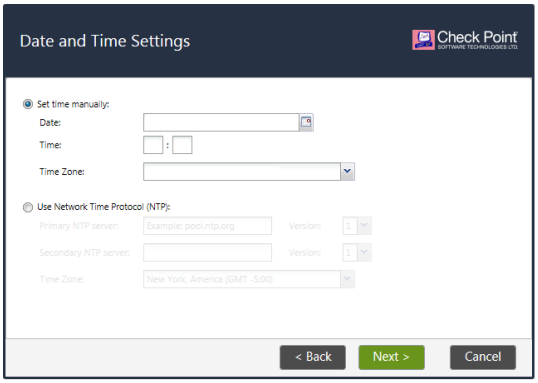
- Verificamos que la información introducida cuando hemos realizado la fresh install es correcta y si no la introducimos de nuevo. Pulsamos "Next" y nos mostrará la página de "Internet Connection".



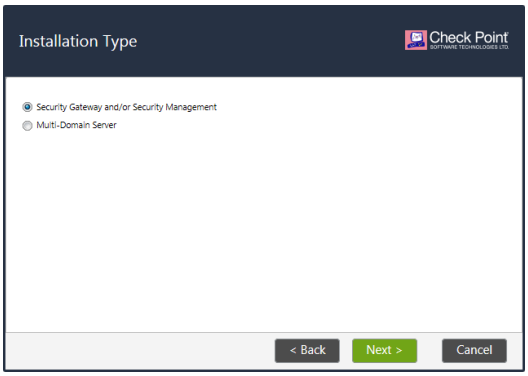
- Pulsamos "Next" y nos dirigiremos hacia la pantalla "Device Information".



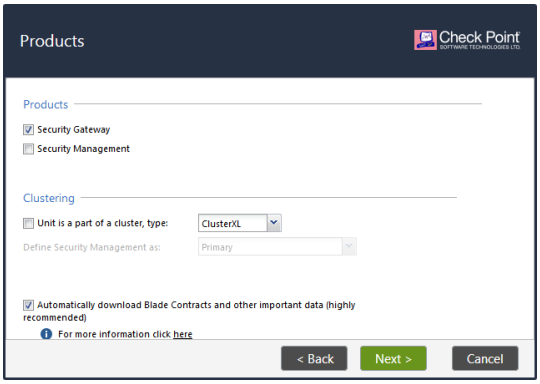
- En esta página rellenamos los campos que necesitemos y pulsamos sobre el botón "Next" que nos llevará a la página "Date and Time Settings".



– En la pantalla de "Date and Time Setting", se puede introducir una configuración manual o bien se puede seleccionar la opción de elegir un servidor NTP. Una vez realiza esta configuración pulsamos el botón "Next" y nos dirigiremos a la pantalla "Installation Type".



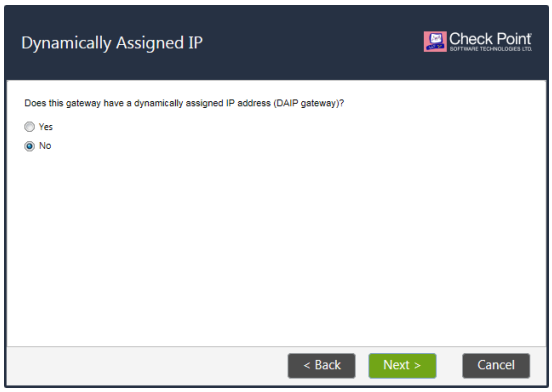
– En la pantalla "Installation Type" seleccionaremos el tipo de instalación que se adecue en función del tipo de despliegue que hayamos implementado. En este caso seleccionaremos la opción "Security Gateway and/or Security Management" y pulsaremos el botón "Next" que nos llevara a la pantalla "Products".



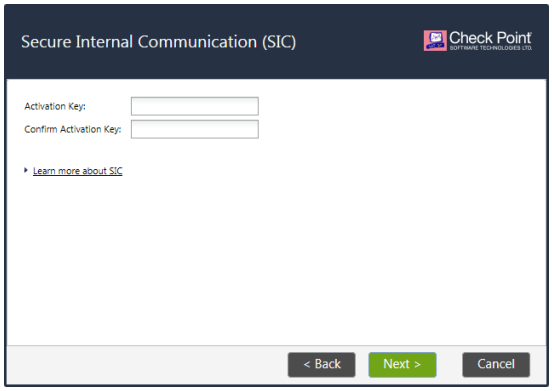
– En esta pantalla se puede seleccionar diferentes opciones:

- **Security Gateway**, si vamos a realizar un despliegue de tipo distribuido y este equipo va a utilizarse como *Gateway*, además si va a ser uno de los nodos de un *Cluster* deberemos seleccionar "Unit is a part of a cluster, type"**.**
- **Security Management,** si vamos a realizar un despliegue de tipo distribuido y este equipo va a utilizarse como *Security Management*.
- **Security Gateway + Security Management,** para despliegue *Standalone*.

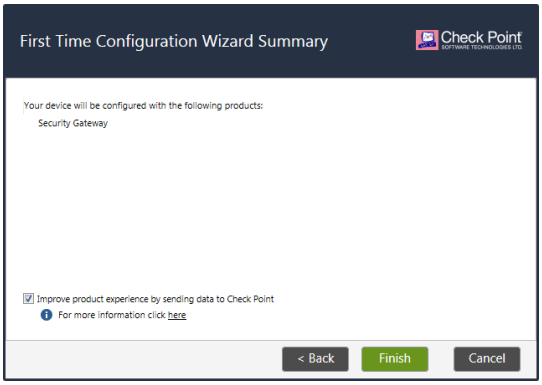
– En nuestro caso seleccionamos el botón Security Gateway y pulsamos “Next”, nos llevara a la pantalla “*Dynamically Assigned IP*”.



– Seleccionar la opción que necesitemos y pulsaremos en el botón “Next”, nos llevara a la pantalla “Secure Internal Communication” (SIC).

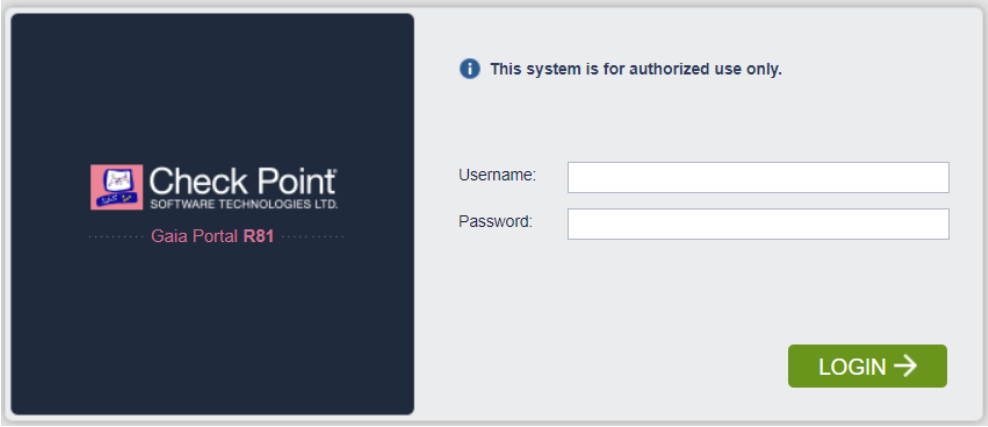


– En esta pantalla introducir la *Activation Key* y la confirmamos. Tras introducir esta pulsar sobre el botón “Next” y llevara a la pantalla de “Summary”.



– Pulsar en “Finish” y el sistema preguntará si desea iniciar la configuración. Pulsar en “Yes”.

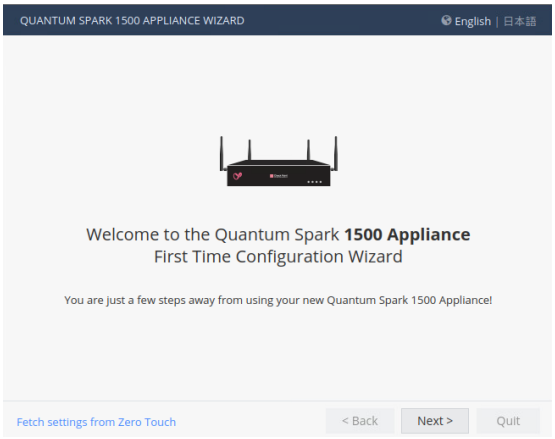
– Una vez que se completa el proceso de configuración, el sistema mostrará un mensaje de reinicio. Pulsar “OK”, y el sistema mostrará la pantalla de inicio de sesión después de reiniciar.



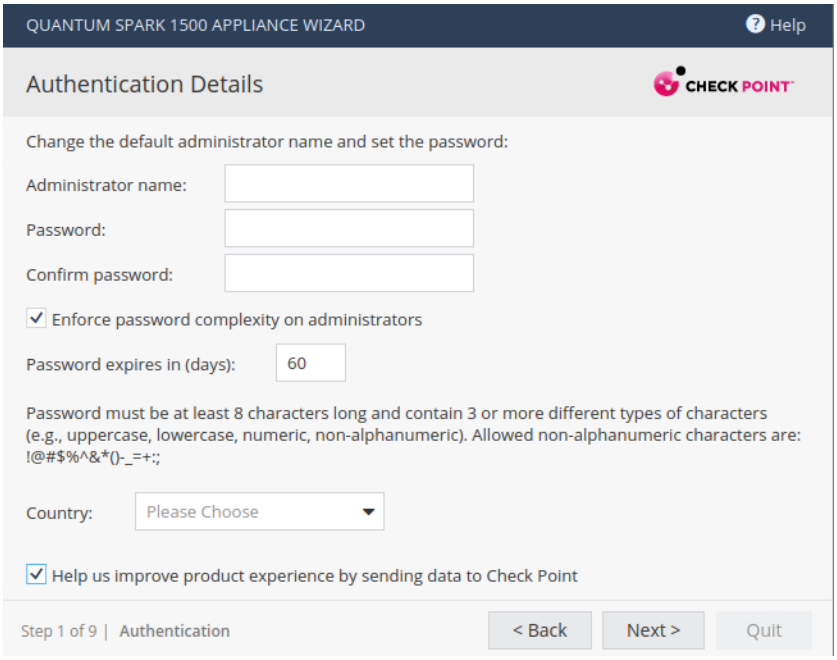
7.1.2 QUANTUM SPARK

Iniciamos un navegador de Internet, como Firefox o Internet Explorer.

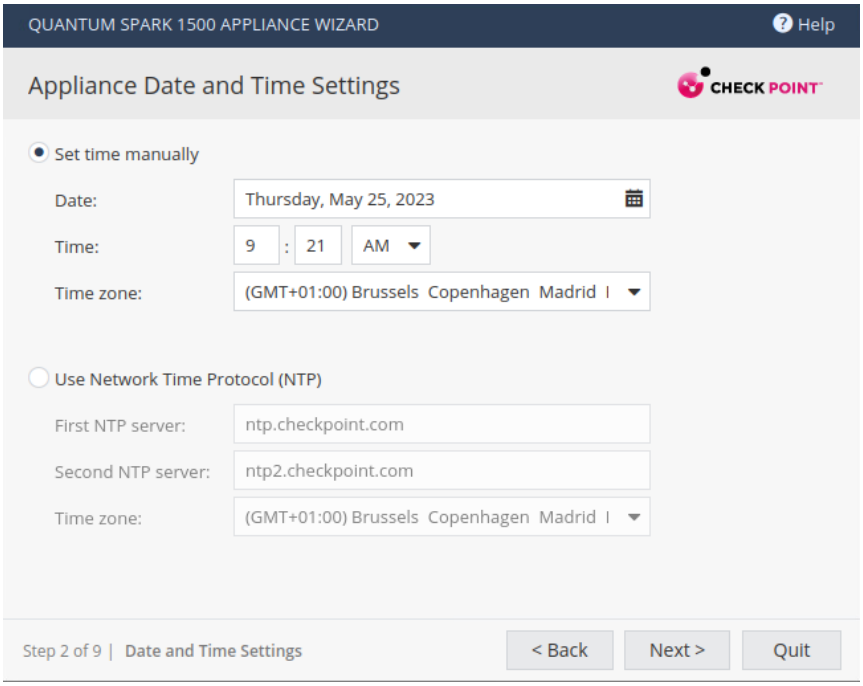
- En el campo de dirección escriba lo siguiente: https://192.168.1.1
- Presionar “Entrar” y el navegador debe advertir que el Certificado de seguridad del sitio no es de confianza.
- Ignorar esta advertencia y continuar con la pantalla de configuración inicial.



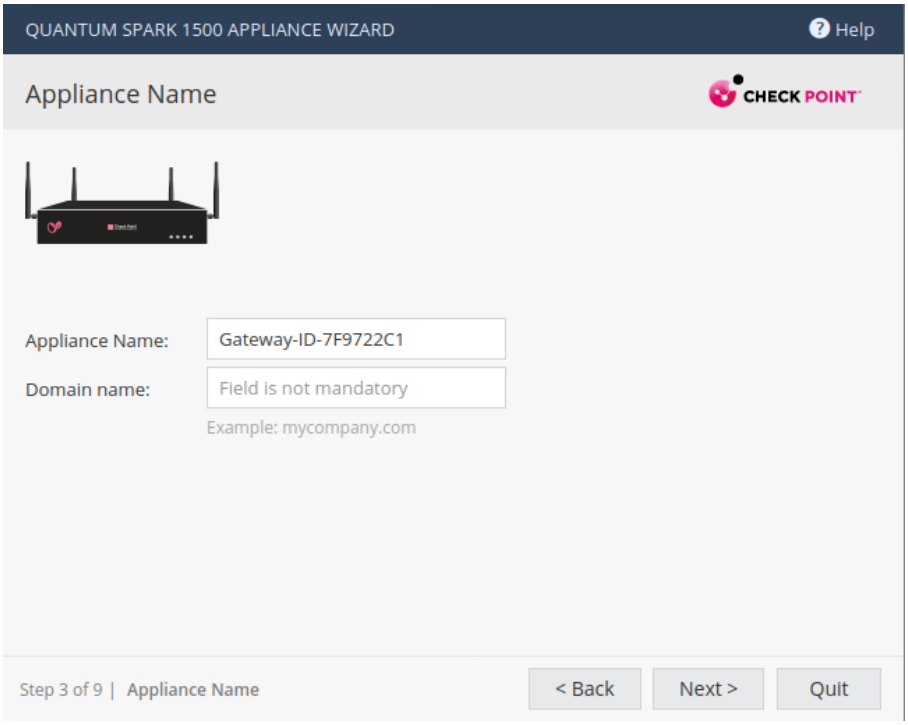
- Pulsar en “Next”, el sistema mostrará la pantalla para configurar la autenticación del dispositivo.



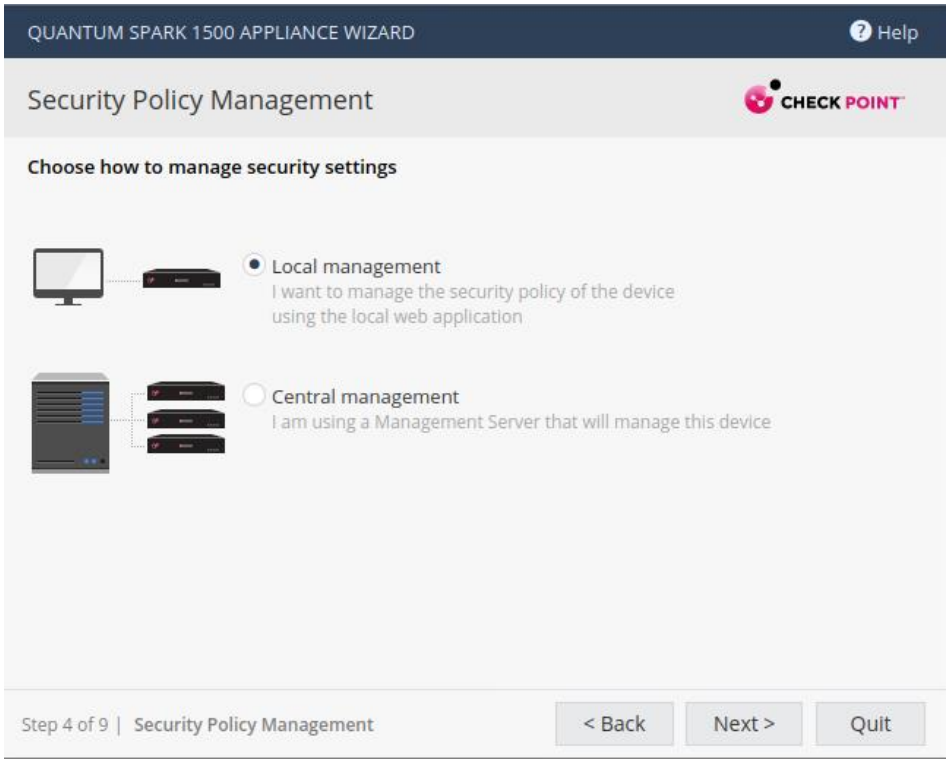
- Será necesario marcar la opción "Enforce password complexity on administrators" y establecer 60 días como plazo de expiración de la clave ("Password expires in").
- Introducimos los datos para crear una cuenta de administrador. Pulsamos "Next y nos mostrará la pantalla de "Appliance Date and Time Settings".



- En la pantalla de "Appliance Date and Time Setting", se puede introducir una configuración manual o bien se puede seleccionar la opción de elegir un servidor NTP. Una vez realiza esta configuración pulsamos el botón "Next" y nos dirigiremos a la pantalla "Appliance Name".

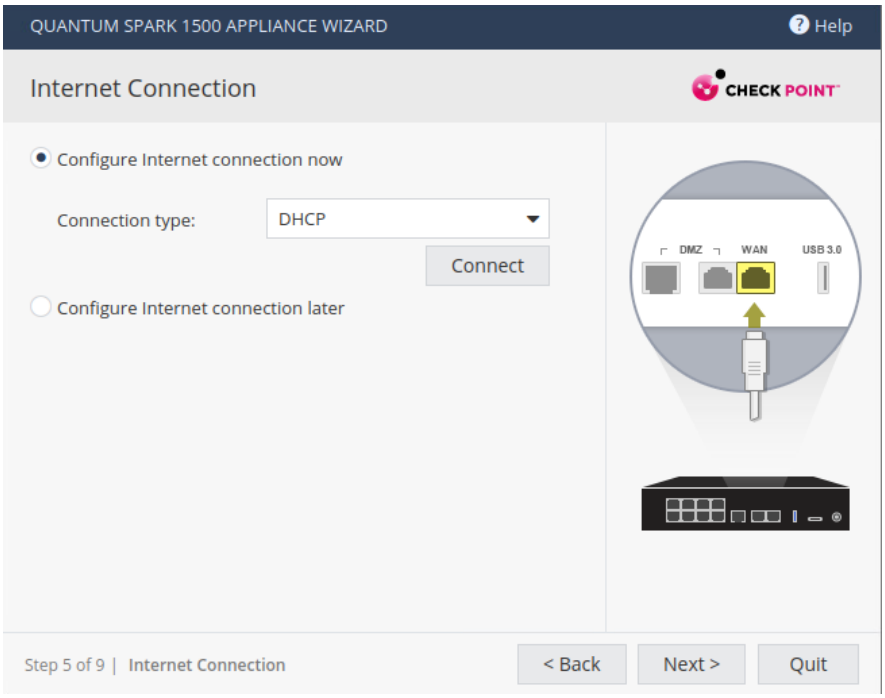


– En esta pantalla rellenamos los campos que necesitemos y pulsamos sobre el botón "Next" que nos llevará a la pantalla "Security Policy Management".

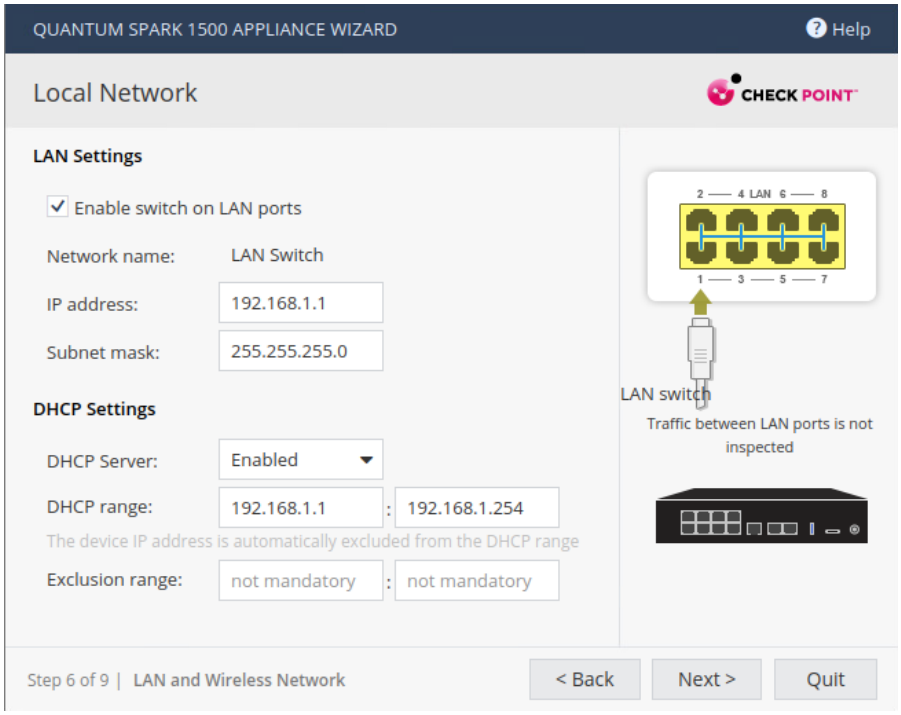


– En la pantalla de "Security Policy Management" seleccionamos el tipo de gestión que se quiere configurar. Es posible configurar dos métodos distintos, "Local management" para gestionar la configuración desde la interfaz web del dispositivo y "Central management" para gestionar la configuración de manera centralizada desde un Security Management. Para alcanzar el modo de operación seguro se deberá

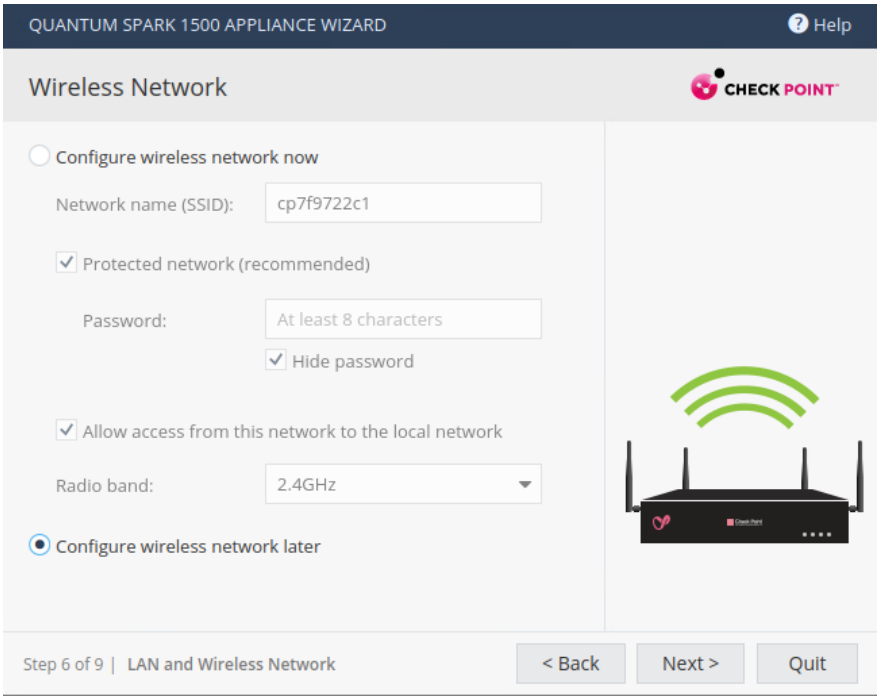
seleccionar la opción “Central Management”. Pulsamos “Next” que nos llevara a la pantalla “Internet Connection”.



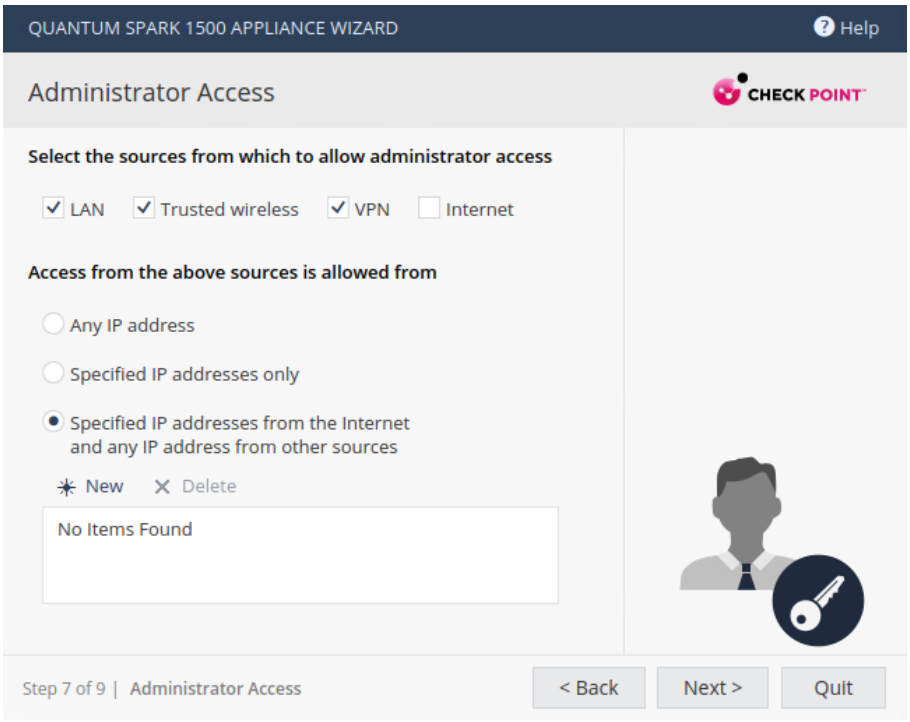
– Configuramos la interfaz WAN o bien dejamos dicha interfaz sin configurar, pulsamos “Next” y nos mostrará la pantalla de “Local Network”.



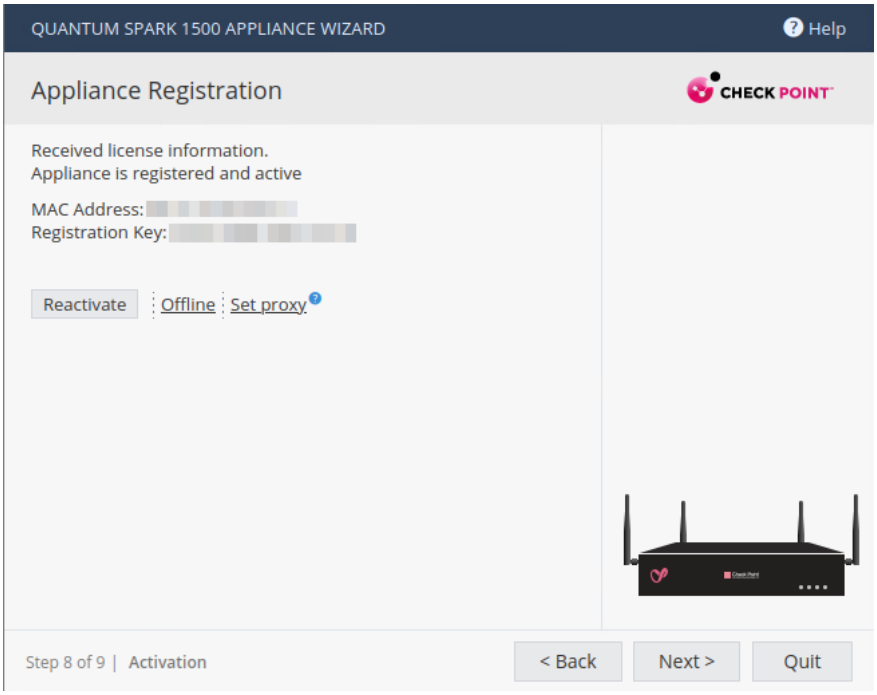
– En la pantalla de “Local Network” definimos la configuración deseada para los puertos de área local y pulsamos “Next”, esto nos llevará a la pantalla de “Wireless Network”.



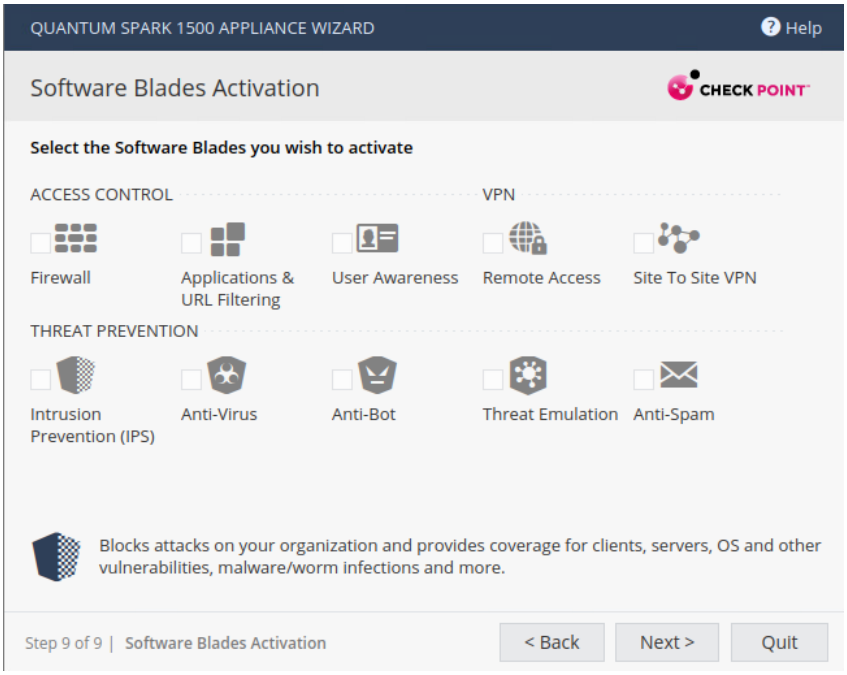
– En la pantalla "Wireless Network" es posible definir una red inalámbrica o bien mantenerla deshabilitada. Una vez realizada esta configuración pulsamos el botón "Next" y nos dirigiremos a la pantalla "Administrator Access".



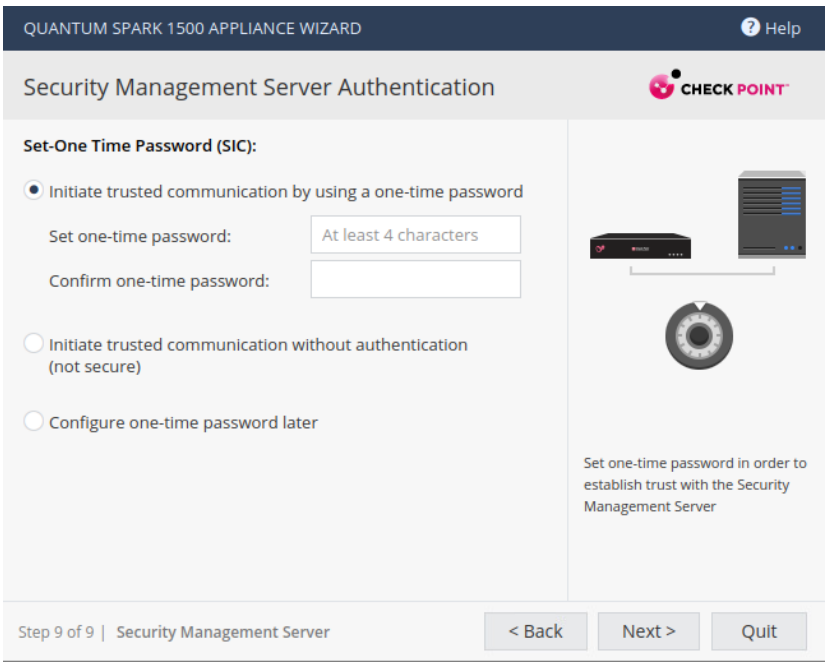
– Desde la pantalla "Administrator Access" es posible restringir el acceso de los administradores desde distintas interfaces o direcciones IP. Una vez configurado pulsaremos el botón "Next" que nos llevará a la pantalla "Appliance Registration".



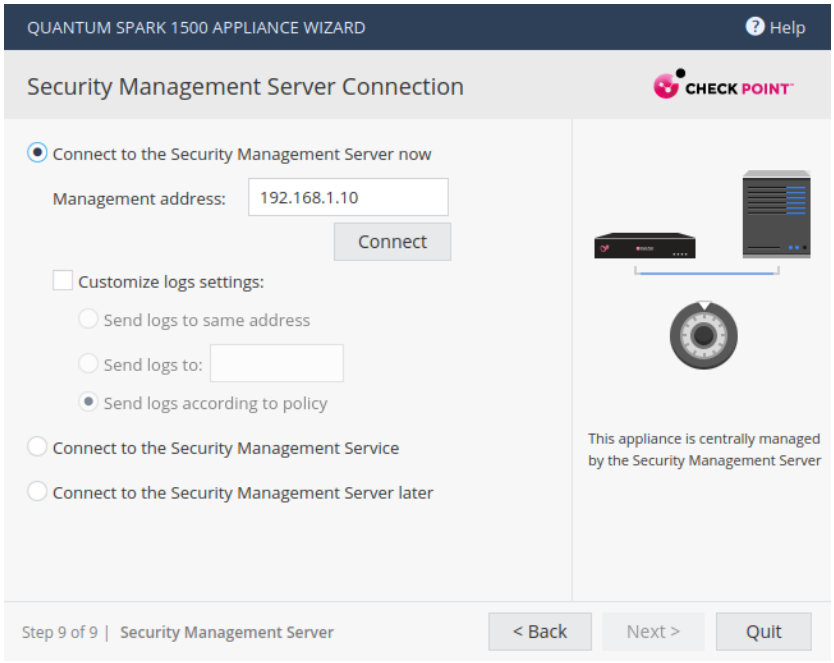
- En la pantalla “Appliance Registration” se lleva a cabo la activación del dispositivo. En caso de disponer de conexión a Internet se puede pulsar “Activate” o “Reactivate” para obtener la licencia de manera automática, en caso de no disponer de acceso a Internet presionar “Offline” para realizar la activación mediante un fichero de licencia. Tras activar el dispositivo pulsar “Next” lo cual nos llevará a la siguiente pantalla.
- En caso de haber seleccionado previamente “Local management” para la gestión nos llevará a la pantalla de “Software Blades Activation”, en caso de haber seleccionado “Central management” nos llevará a la pantalla “Security Management Server Authentication”.



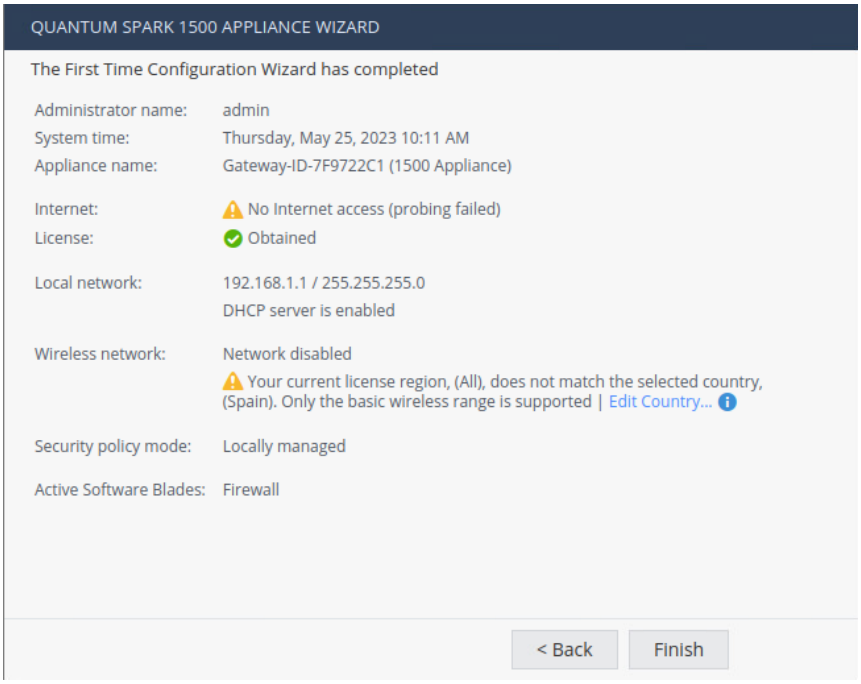
– En la pantalla “Software Blades Activation” es posible seleccionar todos los Software Blades que se desean activar en el dispositivo. Tras pulsar “Next” nos mostrará una pantalla indicando que la configuración inicial ha sido completada.



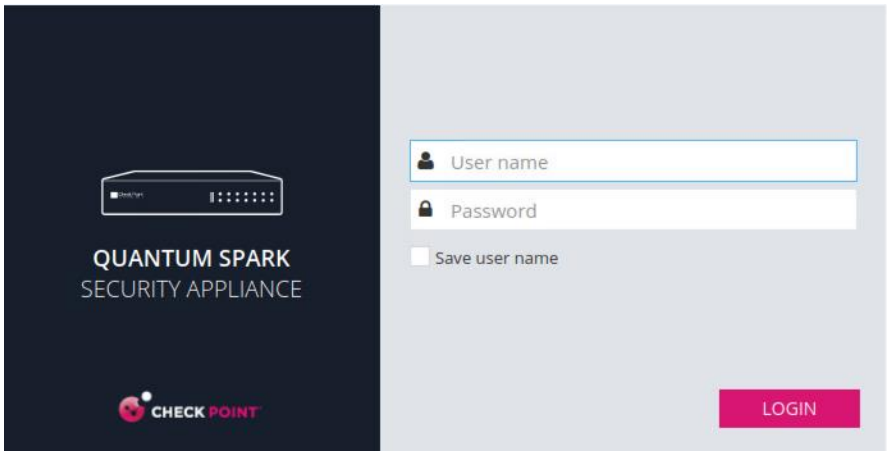
– En la pantalla “Security Management Server Authentication” se establece la contraseña que se utilizará para la autenticación con el Security Management. Tras introducir la contraseña pulsar “Next”, esto nos llevará a la pantalla “Security Management Server Connection”.



– La pantalla “Security Management Server Connection” permite definir la dirección IP del Security Management, al pulsar el botón “Connect” el dispositivo establece la conexión con el Security Management para la obtención de políticas. Tras pulsar “Next” nos mostrará una pantalla indicando que la configuración inicial ha sido completada.



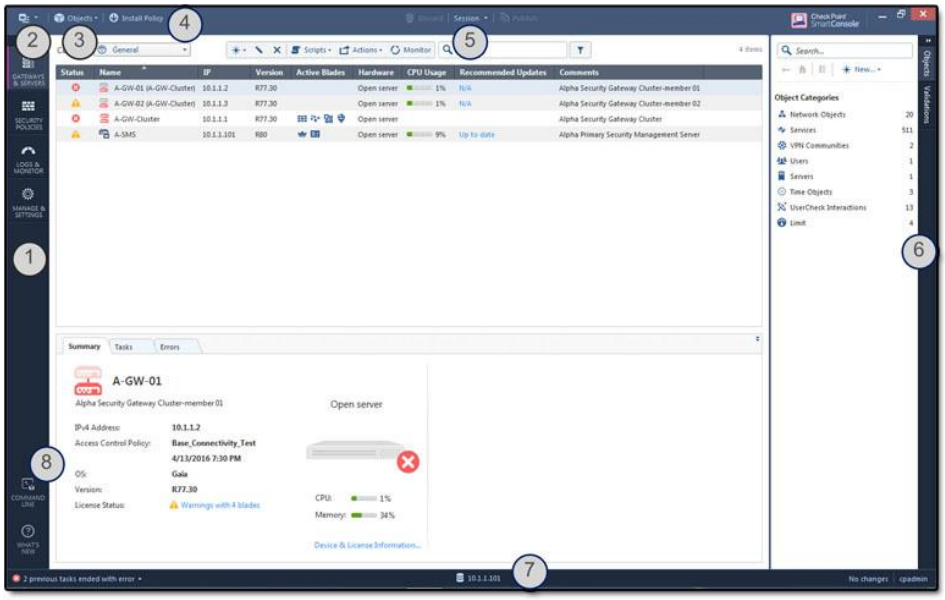
- Pulsar en “Finish” y el sistema preguntará si desea iniciar la configuración. Pulsar en “Yes”.
- Una vez que se completa el proceso de configuración, el sistema mostrará un mensaje de reinicio. Pulsar “OK”, y el sistema mostrará la pantalla de inicio de sesión después de reiniciar.



- Tras terminar la configuración inicial será necesario deshabilitar el servidor SSH del dispositivo.
- Acceder por SSH al dispositivo y ejecutar el comando “expert” para acceder la consola avanzada. Ejecutar el comando “vi /pfrm2.0/bin/sshd” para editar la configuración del servidor SSH y remplazar el valor “$p” del parámetro “-p” por “127.0.0.1:$p”.
- Reiniciar el dispositivo.

7.2 SMARTCONSOLE

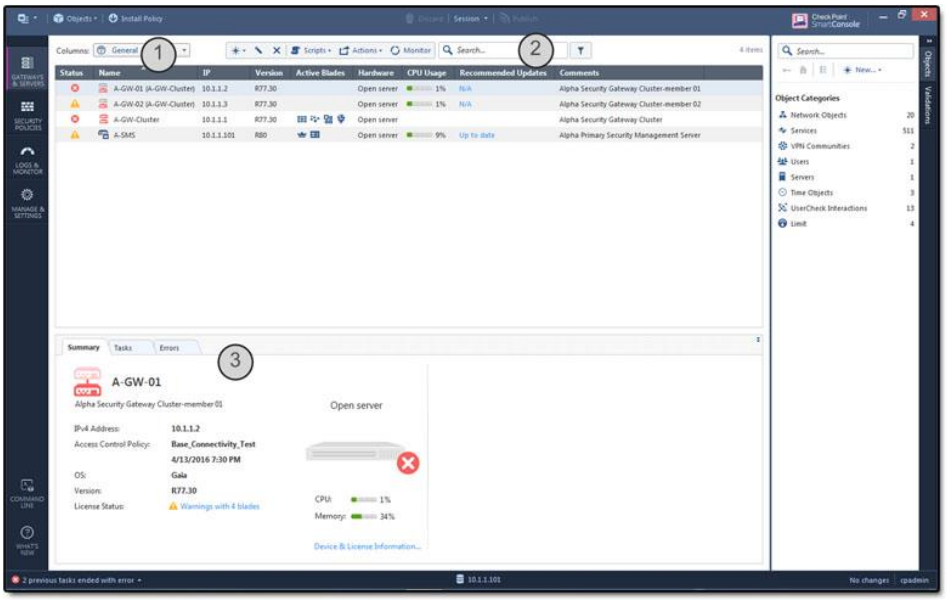
Smartconsole es la consola unificada para gestionar las Políticas de seguridad, monitorizar eventos, instalar actualizaciones, añadir nuevos dispositivos, etc.



- Barra de herramientas: Permite poder navegar entre las distintas vistas.
- Menú principal: Permite administrar políticas y capas, explorar y crear objetos, administrar sesiones, licencias y paquetes, y configurar propiedades globales.
- Menú de objetos: Permite crear y administrar objetos.
- Botón de Instalar política: Permite la instalación de la política de seguridad.
- Detalles de sesión: Ver nombre, descripción y publicar o descartar la sesión.
- Barra lateral: Crear y administrar objetos y visualizar errores de validación.
- Barra actividad de administración: Ver administrador y cambios realizados en la sesión, servidor de administración y tareas de instalación de políticas.
- Línea de comando: Para ejecutar comandos y scripts de API.

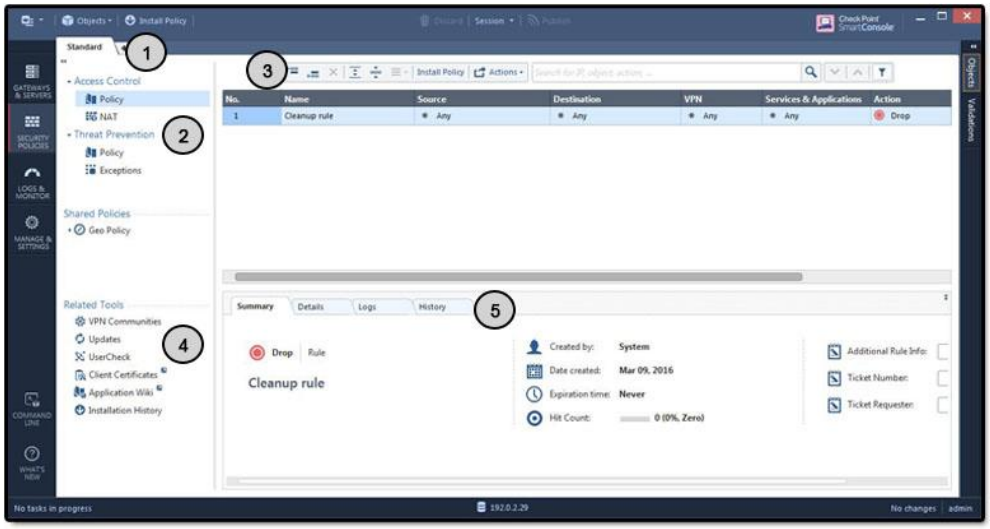
SmartConsole está organizado en las siguientes pestañas:

- **Gateways & Servers:** Para administrar *Gateways*, configurar la activación de *Software Blades* y ver el estado del *Security Gateway/Quantum Spark*:



- Menú de vistas: Para navega entre varias vistas predefinidas.
- Barra de herramientas: Permite crear y editar *Gateways* y C*lúster*, ejecutar scripts, realizar copias de seguridad y restauraciones, y buscar y filtrar puertas de enlace.
- Sección de información adicional: Dónde se puede ver un resumen de la puerta de enlace seleccionada, tareas y mensajes de error y *Software Blades* instalados.

– **Security Policy:** En la pestaña de "Políticas de seguridad", se puede manipular las diversas políticas y capas de seguridad:



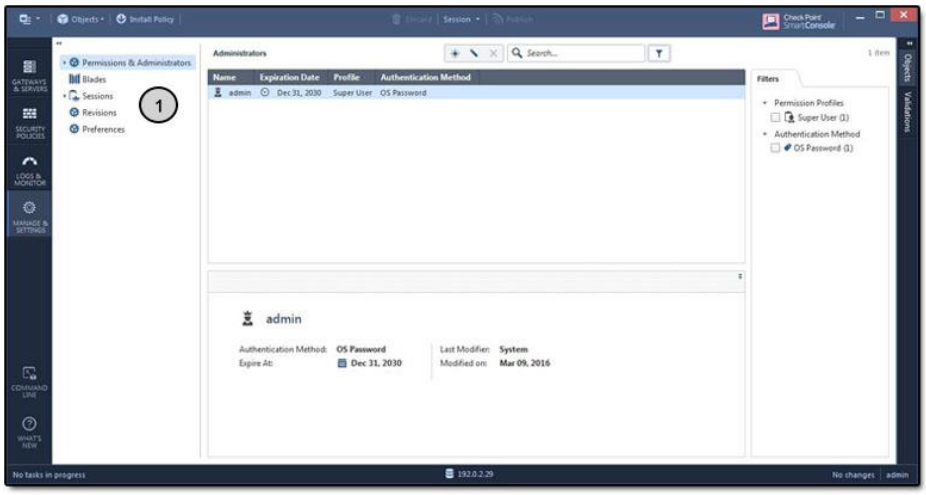
- Pestañas: Permite navegar entre diferentes paquetes de políticas.
- Menú del paquete de políticas: Permite navegar entre varias políticas dentro de un paquete de políticas y visualizar y administrar las políticas compartidas.
- Barra de herramientas: Permite agregar o eliminar reglas, expandir y contraer secciones, instalar políticas, ver el historial y buscar, filtrar y exportar la Base de reglas.

- Herramientas relacionadas: Dónde se puede ver y editar comunidades VPN, actualizaciones, crear y administrar mensajes "UserCheck", administrar certificados de clientes, navegar hasta "Application Wiki" o "ThreatWiki", y ver el historial de instalación.
- Sección de información adicional: Dónde se puede ver un resumen de la regla seleccionada junto con detalles, registros e historial.

– **Logs & Monitor:** La pestaña "Logs & Monitor" le permite ver gráficos y tablas dinámicas, buscar entre registros de *logs*, programar informes personalizables y monitorizar las puertas de enlace.

- Pestañas: Permite abrir varias vistas de análisis de eventos.
- Barra de herramientas: Permite usar consultas predefinidas y personalizadas para buscar registros de logs, actualizar estadísticas, exportar resultados de búsqueda y administrar configuraciones de consultas.

– **Manage & Settings:** La pestaña "*Manage & Settings*" le permite manipular varias configuraciones generales:



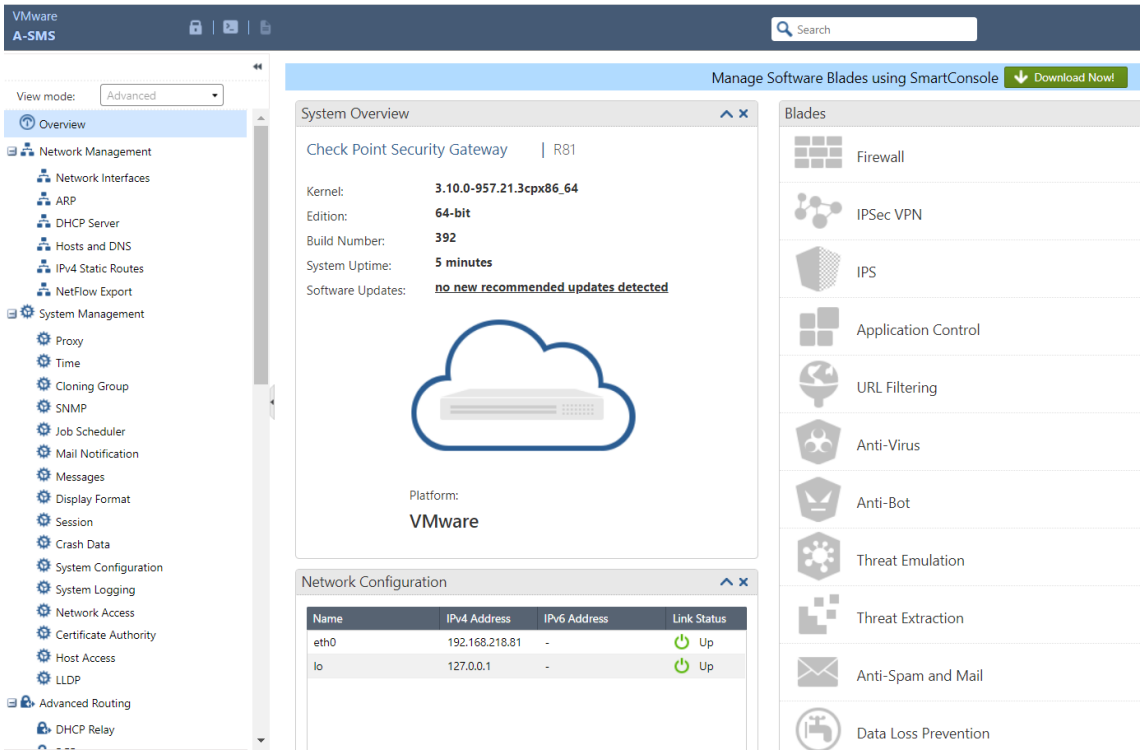
- Menú de administración y configuración: Permite navegar entre las diversas opciones de menú, crear, editar y administrar perfiles de permisos y administradores, administrar las propiedades globales de los Software Blades, ver sesiones y revisiones, administrar etiquetas y editar preferencias, etc.

7.3 WEBUI

WebUI es una interfaz basada en web que se usa para configurar plataformas de Gaia. Proporciona acceso sin cliente a la CLI de Gaia directamente desde un navegador. La mayoría de las tareas de configuración del sistema se pueden realizar a través de WebUI.

Para acceder a WebUI, navegue a: ***https://<Dirección IP del dispositivo>.*** Iniciar sesión con un nombre de usuario y contraseña.

7.3.1 SECURITY GATEWAY



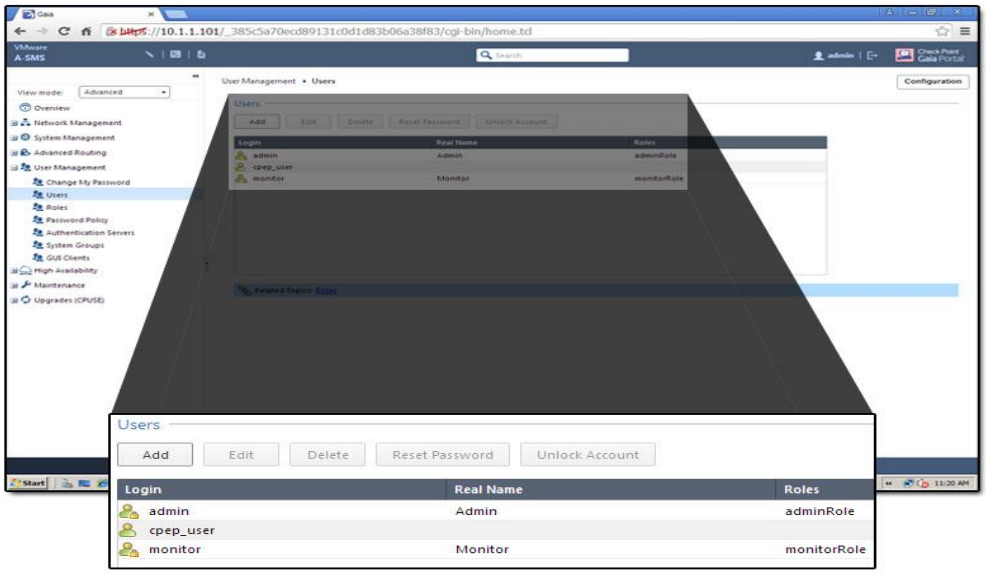
Muestra una descripción general del sistema en varios *widgets*. Estos *widgets* pueden agregarse o eliminarse de la página, moverse por la página y minimizarse o expandirse.

Los siguientes *widgets* están disponibles:

- Descripción general del sistema: Proporciona información del sistema, incluido el producto instalado, el número de versión del producto, la compilación del *kernel*, la compilación del producto, la edición (32 bits o 64 bits), la plataforma en la que está instalado Gaia y el número de serie de la computadora (si corresponde).
- *Software Blades*: muestra una lista de *Software Blades* instalados. Aquellos que están habilitados son de color. Los que no están habilitados aparecen atenuados.
- Configuración de red: muestra interfaces, su estado y direcciones IP.
- Monitor de memoria: proporciona una visualización gráfica del uso de la memoria.
- Monitor de CPU: proporciona una visualización gráfica del uso de la CPU.

WebUI y CLI se pueden usar para administrar cuentas de usuario y realizar las siguientes acciones:

- Agregar usuarios a su sistema Gaia.
- Editar el directorio de inicio del usuario.
- Editar el *shell* predeterminado para un usuario.
- Asignar una contraseña a un usuario.
- Asignar privilegios a los usuarios.



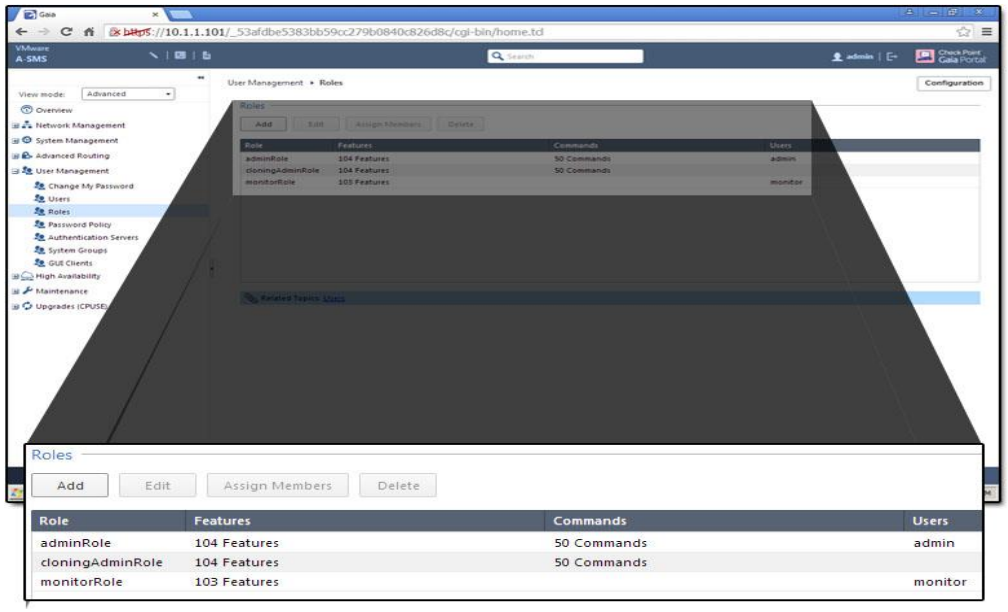
Hay dos usuarios predeterminados que no se pueden eliminar. El *administrador* tiene acceso de lectura/escritura para todas las funciones de Gaia. Este usuario tiene una ID de usuario de 0 y, por lo tanto, tiene todos los privilegios de un usuario raíz. El *monitor* tiene acceso de solo lectura para todas las funciones en la WebUI y la CLI.

Los usuarios nuevos tienen privilegios de solo lectura para WebUI y CLI de forma predeterminada. Se les debe asignar uno o más roles antes de que puedan iniciar sesión.

La administración basada en roles permite a los administradores de Gaia crear diferentes roles. Los administradores pueden permitir a los usuarios acceder a las funciones agregando esas funciones a la definición de rol del usuario.

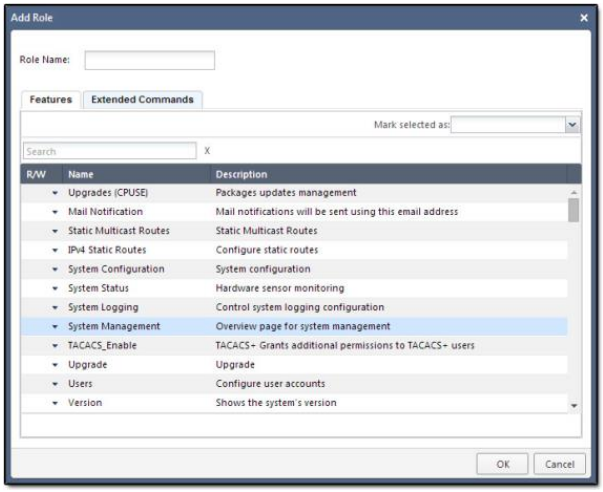
Cuando se crea un usuario, se asignan roles predefinidos o privilegios al usuario. Por ejemplo, un usuario con acceso de lectura/escritura a la función “Usuarios” puede cambiar la contraseña de otro usuario. También es posible especificar qué mecanismos de acceso, WebUI o CLI están disponibles para el usuario.

Cuando los usuarios inician sesión en la WebUI, solo ven aquellas características para las que tienen acceso de solo lectura o de lectura/escritura. Si tienen acceso de solo lectura a una función, pueden ver las páginas de configuración pero no pueden cambiar la configuración.



Los roles se definen en la página "Roles" de la WebUI. Para agregar un nuevo rol o cambiar un rol existente:

- Seleccionar *Administración de usuarios* ➔ *Roles* en el árbol de navegación de WebUI.
- Para agregar un nuevo rol, pulse en "Agregar" e ingrese un nombre de rol. El nombre del rol puede ser una combinación de letras, números y el carácter de subrayado "_", pero debe comenzar con una letra.
- Para cambiar los permisos de un rol existente, pulse dos veces en el rol.
- En la ventana "Agregar" o "Editar" función, pulse en una característica (pestaña "Funciones") o en el comando extendido (pestaña "Comandos extendidos").
- Seleccionar "*None*", "*Read Only*" o "*Read / Write*" en el menú de opciones a la izquierda de la función o comando.



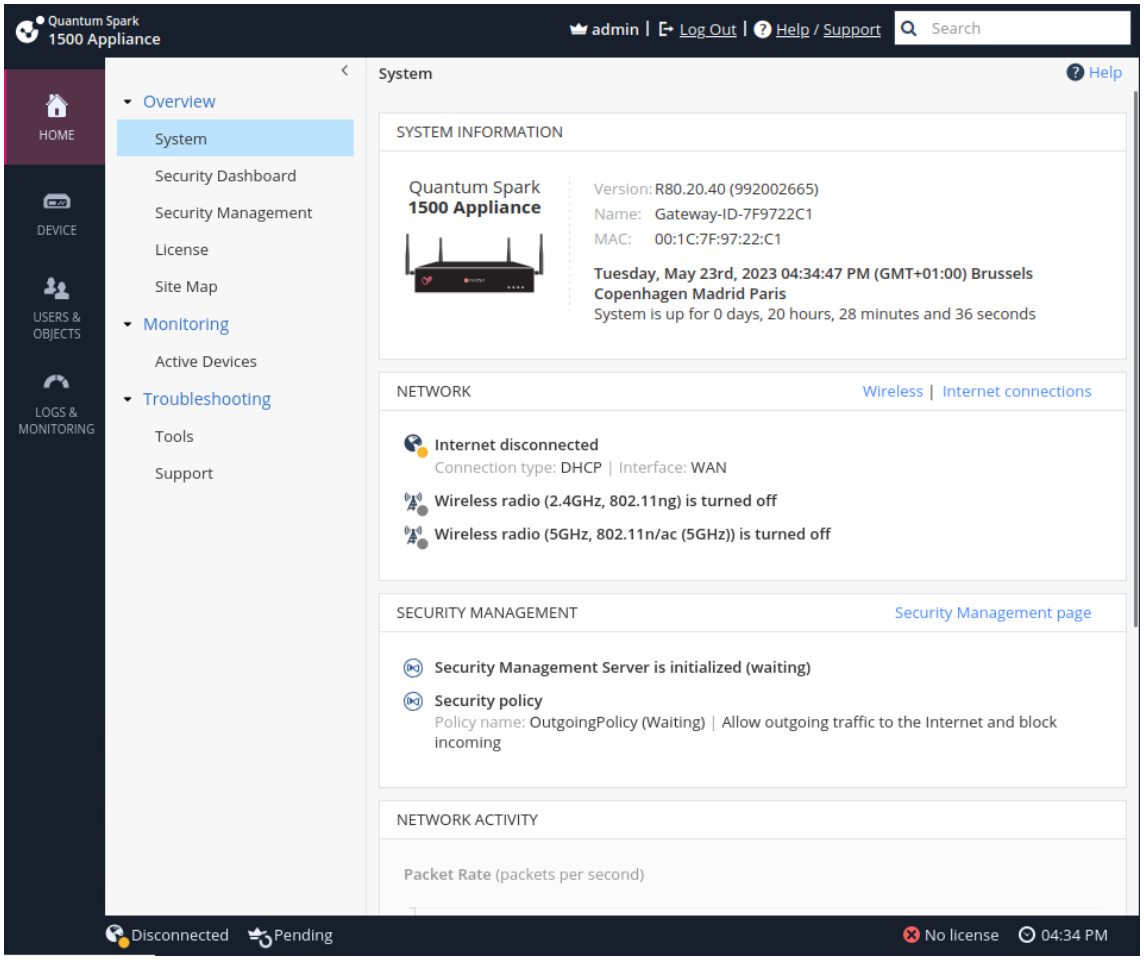
Para asignar usuarios a un rol:

- Seleccionar *Administración de usuarios* ➔ *Roles* en el árbol de navegación de WebUI.
- Pulsar en Asignar miembros.

– En la ventana Asignar miembros a la función:

  - Pulsar dos veces en un usuario en la lista de Usuarios disponibles para agregar ese usuario a la función.
  - Pulsar dos veces en un usuario en la lista Usuarios con rol para eliminar ese usuario del rol.

7.3.2 QUANTUM SPARK



Muestra la información completa del sistema a través de una interfaz basa en pestañas, desde las distintas pestañas es posible visualizar la configuración del dispositivo y realizar cambios. Las pestañas en las que se divide son las siguientes:

- *Home*: Muestra información para comprobar el estado del dispositivo *Quantum Spark* y permite la activación de *Software Blades*.
- *Device*: Posibilita realizar cambios en la configuración propia del dispositivo gestionando interfaces, configuración de alta disponibilidad, fecha y hora…
- *User & Objects*: Permite la gestión de los usuarios del dispositivo y la definición de recursos de red.
- *Logs & Monitoring*: Pestaña desde la cual es posible la visualización de los registros de auditoría generados y la configuración de los servicios de SNMP y reenvío de logs.

- *Pestañas adicionales relativas a los Software Blades:* Cada *Software Blade* activado mostrará una nueva pestaña que permitirá su gestión desde la interfaz web.

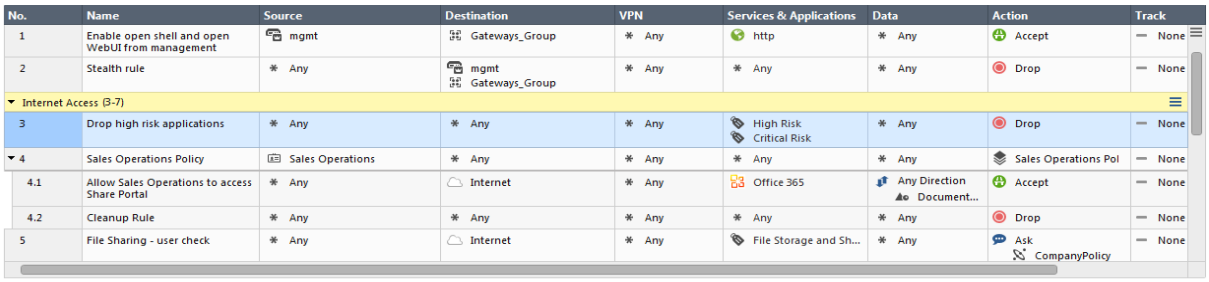
7.4 REGLAS Y POLÍTICAS DEL CORTAFUEGOS

La Política de seguridad es un componente clave para asegurar y administrar cualquier red corporativa, sin importar cómo de grande o pequeña sea.

Una Política de seguridad es una colección de objetos, configuraciones y reglas que controlan el tráfico de la red y aplica las directrices de la organización para la protección de datos y el acceso a los recursos.

Una vez que se define una Base de reglas, la Política de seguridad se puede distribuir a todos los *Security Gateways/Quantum Spark*.

Las reglas están compuestas de objetos de red, como *Security Gateways Quantum Spark*, *hosts*, redes, enrutadores y dominios, y especifican el origen, el destino, el servicio y la acción que se tomarán para cada sesión. Una regla básica consiste en la siguiente información:



- Número de regla.
- Nombre de la regla.
- Fuente.
- Destino.
- Si se usará VPN o no.
- Servicios y aplicaciones.
- Acción a seguir si el criterio de sesión coincide.
- Si se rastrea y cómo debe rastrearse la actividad de la regla.
- En qué objeto u objetos de Firewall se aplicará la regla.
- El período de tiempo para la regla.

7.4.1 REGLA POR DEFECTO

Se añade una regla por defecto cuando el usuario agrega una regla a la Base de reglas. Estas reglas se configuran usando todos los objetos, servicios y usuarios instalados en la base de datos. La regla predeterminada se define con la siguiente información:

No.	Name	Source	Destination	VPN	Services & Applicat...	Action	Track	Install On	Time
1	NEW	Any	Any	Any	Any	Drop	None	Policy	Any
2	Cleanup rule	Any	DMZZone DMZNet	Any	Any	Accept	None	Policy	Any

- No.: Define el orden numérico de cada regla; la primera regla es 1.
- Hits: Realiza un seguimiento del número de conexiones en cada regla.
- Nombre: Da a los administradores un espacio para poner un nombre a la regla.
- Origen: Muestra el selector de objetos, donde puede seleccionar objetos de red o un grupo de usuarios para agregar a la Base de reglas; el valor predeterminado es “Any”.
- Destino: Muestra el selector de objetos, donde puede seleccionar objetos de recursos para agregar a la regla; el valor predeterminado es “Any”.
- VPN: Muestra como agregar comunidades VPN, donde puede seleccionar una Comunidad VPN para agregar; el valor predeterminado es “Any”.
- Servicios y aplicaciones: Muestra el selector de Servicios y aplicaciones, donde puede seleccionar servicios para agregar a la regla; el valor predeterminado es “Any”.
- Acción: Aceptar, descartar o rechazar la sesión. Proporciona autenticación y encriptación; el valor predeterminado es “Drop”.
- Seguimiento: Define el registro o las alertas para esta regla; el valor predeterminado es “None”. Las opciones son*: None, Network Log, Log, Full Log, Accounting, Suppression,* y *Alert*.
- Instalar en: Especifica en qué objetos de Firewall se hará cumplir la regla; el valor predeterminado es “Policy Targets”, lo que representa a todos los objetos internos de *Firewall*.
- Tiempo: Especifica el periodo de tiempo para la regla; el valor predeterminado es “Any”.
- Comentario: Permite a los administradores agregar notas sobre esta regla.

7.4.2 OBJECTOS

En *SmartConsole*, los objetos se utilizan para representar componentes físicos y virtuales de red, como puertas de enlace, servidores y usuarios, así como componentes lógicos como servicios (HTTP y TELNET) y recursos (URI y FTP). Los componentes lógicos incluyen rangos de direcciones IP y objetos dinámicos.

Los objetos se dividen en las siguientes categorías:

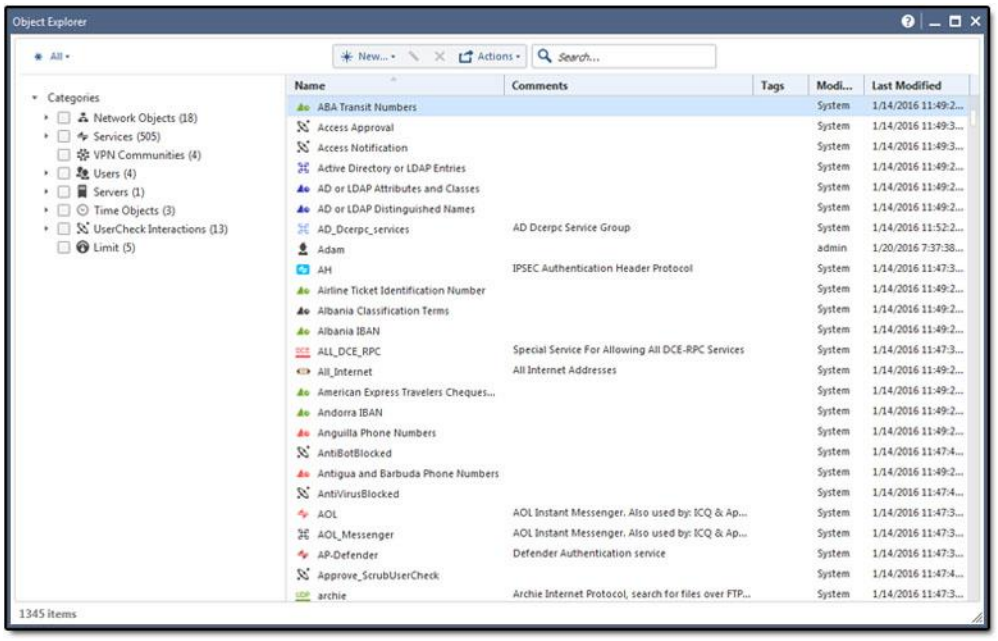
- ***Network objects***: *Security Gateways/Quantum Sparks*, *hosts*, redes, rangos de direcciones, objetos dinámicos, zonas de seguridad, dominios y servidores lógicos.
- ***Service***: Protocolos y grupos de protocolo.
- ***Custom Application/Site***: Aplicaciones, categorías de usuarios y categorizaciones de URLs.
- ***VPN Community***: “VPNs site to site” o de acceso “remote”.
- ***User***: Usuarios, grupos de usuarios, plantillas de usuario.
- ***Server***: Autoridades de certificación de confianza, RADIUS, TACACS, servidores OPSEC.
- ***Resource***: URI de recursos, SMTP, FTP, TCP, CIFS.

- ***Time Object***: Tiempo, *slots* de tiempo, límite de ancho de banda en las tasas de carga y descarga.
- ***UserCheck Interactions***: Ventana de mensajes que se le muestra al usuario (Preguntar, Cancelar, Plantilla de certificado, Informar y Soltar).
- ***Limit***: Limitar el ancho de banda (*download* y *upload*).

Cada componente de una organización tiene un objeto correspondiente que lo representa. Una vez que se crean estos objetos, se pueden usar en las reglas de la Política de seguridad. Los objetos se almacenan en la base de datos de objetos en *Security Management Server*.

Los administradores del sistema pueden agregar, editar, eliminar y clonar objetos. Un clon es una copia del objeto original con un nombre diferente.

La ventana del Explorador de objetos en *SmartConsole* le permite crear objetos nuevos y editar objetos existentes. Desde esta ventana, puede buscar objetos por categorías o buscar un objeto particular usando palabras clave o etiquetas. Una etiqueta es una palabra clave o etiqueta asignada a un objeto o grupo de objetos.

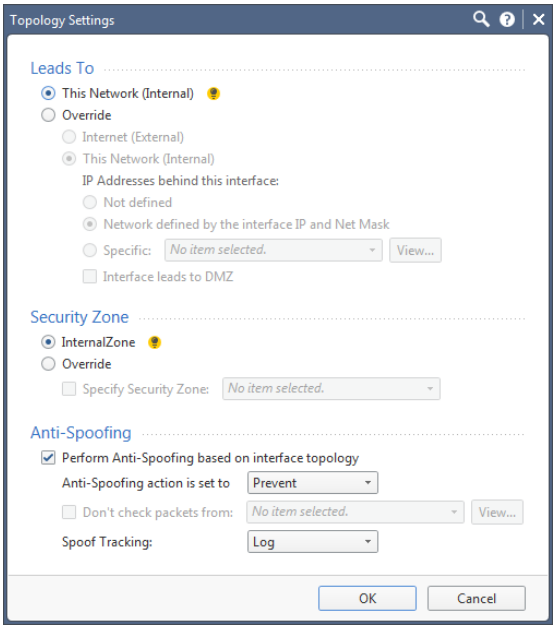


7.4.3 ZONAS DE SEGURIDAD

Una zona de seguridad es un grupo de una o más interfaces de red unidas y usadas directamente en la Base de reglas. Permiten a los administradores definir la Política de seguridad basada en interfaces de red en lugar de direcciones IP.

La zona de seguridad se puede combinar en una regla como zona de origen o zona de destino. El uso de la zona correcta para una conexión dada se basa en la topología de la red.

Una interfaz determinada sólo puede ser parte de una única zona. Las zonas de seguridad externas, internas y DMZ están siempre disponibles en el *Security Gateway/ Quantum Spark* de forma predeterminada.



7.4.4 ANTI-SPOOFING

Spoofing es una técnica en la que un intruso intenta obtener acceso no autorizado alterando la dirección IP de un paquete. Esta alteración hace que parezca que el paquete se originó en la parte de una red con mayores privilegios de acceso. *Security Gateway/ Quantum Spark* tiene una funcionalidad *Anti-Spoofing* que detecta dichos paquetes al requerir que la interfaz por la que un paquete entra a un *Gateway* corresponda a su dirección IP.

Anti-Spoofing verifica que los paquetes provienen de, y van a, las interfaces correctas. Y confirma que los paquetes que afirman ser de la red interna en realidad provienen de la interfaz de red interna, es una configuración de objeto que cuando se configura afecta la política de seguridad

7.4.5 RULE BASE

La Base de reglas es una colección de reglas individuales que crea la política de seguridad. Se aplica la primera regla que coincide con un paquete y se toma la acción especificada. La comunicación puede registrarse mediante un log y/o emitir una alerta, dependiendo de lo que se haya ingresado en el campo “Track”. El concepto fundamental de Base de reglas es "se niega una conexión que no está permitida explícitamente".

7.4.6 CLEANUP Y STEALTH RULE

Hay dos reglas básicas que recomienda Check Point para crear una Política de seguridad efectiva: la regla de “Cleanup” y la regla de “Stealth”. Son importantes para crear medidas de seguridad básicas y rastrear información importante:

- ***Regla de “Cleanup”***: Se recomienda este tipo de regla para determinar cómo gestionar las conexiones que no coinciden con las reglas anteriores de la Base de reglas. También es necesario para registrar mediante *logs* este tráfico. Siempre debe colocarse en la parte inferior de la Base de reglas.

- ***Regla de "Stealth"***: Para evitar que los usuarios se conecten directamente a la puerta de enlace. El *Security Gateway/ Quantum Spark* se vuelve invisible para los usuarios de la red. En la mayoría de los casos, debemos colocar dicha regla en la parte superior de la Base de reglas y así proteger la puerta de enlace del escaneo de puertos, suplantación de identidad y otros tipos de ataques directos.

7.4.7 REGLAS EXPLÍCITAS E IMPLICITAS

Security Management Server crea reglas explícitas e implícitas. El administrador crea reglas explícitas en la Base de Reglas. Las reglas explícitas están configuradas para permitir o bloquear el tráfico según criterios específicos.

Las reglas implícitas están definidas por *Security Gateway/Quantum Spark* para permitir ciertas conexiones hacia y desde *Security Gateway/Quantum Spark*. Las reglas implícitas no son visibles en la Base de reglas por defecto. *Security Management Server* impone dos tipos de reglas implícitas que permiten controlar las conexiones y los paquetes salientes.

El *Security Gateway/Quantum Spark* crea un grupo de reglas implícitas que ubica en primer lugar, en último lugar o antes del último lugar en la Base de reglas explícitamente definidas. Estas primeras reglas implícitas se basan en la configuración. como por ejemplo aceptar conexiones de control. El *Gateway* anticipa conexiones posibles relacionadas con la comunicación del *Gateway* y crea reglas implícitas para esos escenarios.

Hay tres tipos de conexiones de control definidas por reglas predeterminadas:

- Tráfico específico de Gateway que facilita la funcionalidad, como el log, la gestión y el intercambio de claves.
- Aceptación de intercambio de claves de Internet (IKE) y tráfico RDP para fines de comunicación y cifrado.
- Comunicación con varios tipos de servidores, como RADIUS, CVP, UFP, TACACS, LDAP y Servidores lógicos.

Las reglas implícitas se generan en la Base de reglas como parte de las Propiedades globales y no se pueden editar. Están configuradas para permitir conexiones de diferentes servicios que usa el *Security Gateway/Quantum Spark*, como la conexión a servidores de autenticación RADIUS y el envío de logs desde *Security Gateway/Quantum Spark* al *Security Management Server*.

Algunas reglas implícitas están habilitadas por defecto.

7.4.8 PUBLICAR CAMBIOS

Las Políticas de seguridad recién creadas y los cambios realizados en una Base de reglas existente deben publicarse en el servidor de administración antes de que la política se pueda instalar y aplicar en el *Security Gateway/Quantum Spark*.

Publicar cambios no es lo mismo que guardar cambios. Al guardar los cambios realizados durante una sesión en *SmartConsole*, se crea un borrador de la política editada en el servidor de gestión. Los cambios no se actualizan a la política cuando se ven en *SmartConsole*. La política no se instala si los cambios no se publican.

La publicación realmente actualiza la política en el servidor de administración y/o el servidor de registro y hace que los cambios sean visibles en *SmartConsole*. Para publicar la política, simplemente se debe pulsar en el botón "Publish" ubicado en la parte superior de la ventana de *SmartConsole*. Aparecerá una ventana emergente. Se debe pulsar en el botón "Publicar" para que los cambios sean visibles para todos y se actualice la política.

7.4.9 PAQUETE DE POLÍTICAS

Un paquete de políticas es un grupo de diferentes tipos de políticas que se instalan juntas en los mismos objetivos de instalación. Después de la instalación, *Security Gateway/Quantum Spark* aplica todas las políticas del paquete.

Algunas circunstancias requieren múltiples versiones de una Política de Seguridad, sin embargo, la base de datos de Objetos debe permanecer igual. A menudo, esto ocurrirá al agregar o consolidar reglas en una Base de reglas existente o al crear un nuevo conjunto de reglas en un *Security Gateway/Quantum Spark*. En estos casos, usar paquetes de políticas es mejor que crear múltiples versiones de la base de datos del sistema. Los objetivos de instalación predefinidos permiten que cada paquete de políticas se asocie con el conjunto apropiado de puertas de enlace, eliminando así la necesidad de repetir el proceso de selección de la puerta de enlace cada vez que se instalar el paquete.

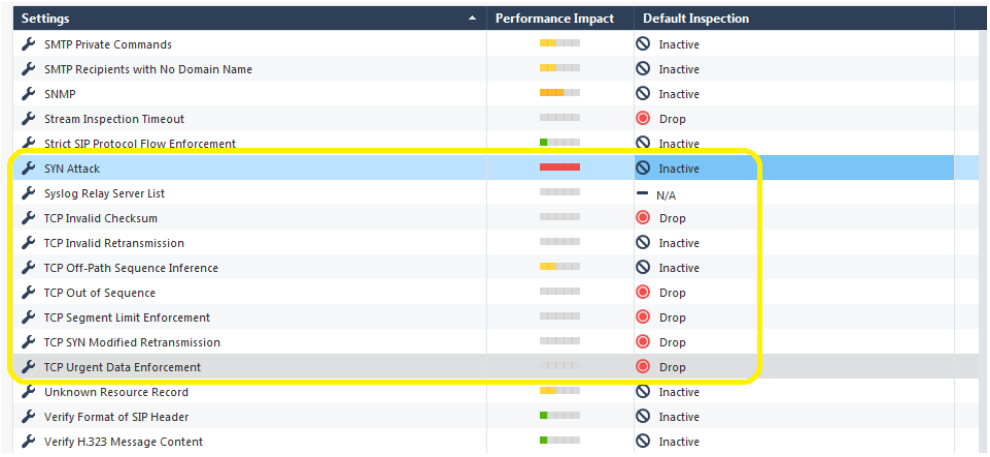
7.4.10 PROTECCIONES DE RED (INSPECTION SETTINGS)

En la configuración del firewall existe lo que se conoce como *Inspections Seting* que permite:

- Inspección profunda de paquetes.
- Inspección de análisis de protocolo.
- Inspección de paquetes VoIP.

Por ejemplo, el no cumplimiento de protocolos, u otras protecciones como SYN ATTACK y paquetes TCP invalidos.

Settings	Performance Impact	Default Inspection
Non Compliant HTTP		Inactive
Non Compliant POP3		Inactive
Non Compliant MSNMS		Inactive
Non-TCP Flooding		Inactive
Non Compliant MS-RPC		Inactive
Non Compliant PPTP		Inactive
Non Compliant SMTP		Inactive
Non Compliant CIFS		Inactive
Non Compliant IMAP		Inactive
Non Compliant DNS		Inactive
Non HTTP Traffic on HTTP Port		Inactive



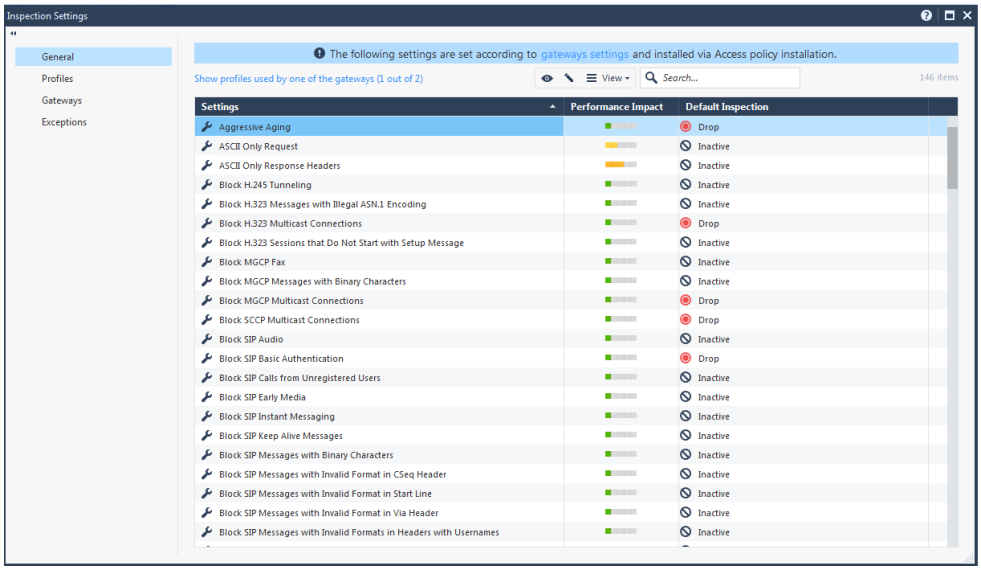
El *Security Management Server* viene con dos perfiles de inspección preconfigurados:

- Inspección por defecto.
- Inspección recomendada.

Para hacer efectivos cambios en la configuración de *Inspection Setting*, es necesario instalar la Política de control de acceso.

Para configurarlo:

- En SmartConsole, ir a Manage & Settings ➔ Blades view.
- En la sección "General", pulse en "Inspection Setting" para abrir la ventana correspondiente.

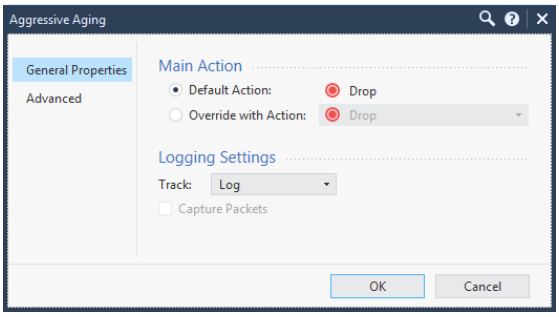


Es posible:

- Editar perfiles de configuración de inspección definidos por el usuario. No se puede cambiar el perfil de inspección predeterminado y el perfil de inspección recomendado.
- Asignar perfiles de configuración de inspección a los *Security Gateways/Quantum Spark*.
- Configurar excepciones a la configuración.

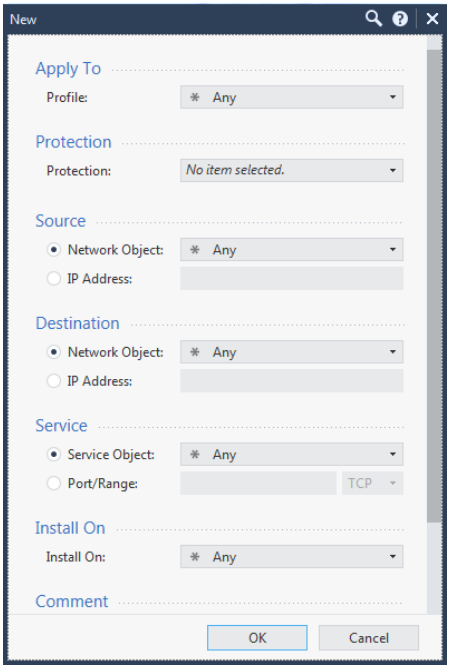
Para editar una configuración:

- En Inspection Settings ➔ General view, seleccione una protección (setting).
- En la ventana que se abre, seleccione un perfil y pulse en "Editar". Se abrirá la ventana de configuración.



- Seleccionar la acción principal:
  - ***Default Action***: Acción preconfigurada.
  - ***Override with Action***: En el menú desplegable, seleccione una acción para anular la opción predeterminada: Accept, Drop, Inactive (la configuración no está activada).
- Configurar "*Logging Setting*" seleccionando "*Capture Packets*" si desea poder examinar los paquetes que fueron bloqueados en las reglas de Drop.
- Pulsar en Aceptar y Cerrar.

Para configurar excepciones: En *Inspection Settings* ➔ *Exceptions*, pulse en añadir una nueva excepción o en modificar una existente.



- ***Apply To:*** Seleccionar el perfil al que aplicar la excepción.
- ***Protection***: Seleccionar la protección (setting) correspondiente.

- ***Source***: Seleccionar el objeto de red de origen o seleccione Dirección IP e ingrese la dirección IP de origen.
- ***Destination***: Seleccionar el objeto de destino.
- ***Service***: Seleccionar Puerto/Rango, TCP o UDP, e ingrese un número de puerto de destino o un rango de números de puerto. O también podrá seleccionar un objeto servicio.
- ***Install on:*** Seleccionar una puerta de enlace en la que instalar la excepción.
- Pulsar en Aceptar.

Para hacer cumplir los cambios, instalar la Política de Control de Acceso.

7.4.11 PROTECCIÓN FRENTE ATAQUES DDOS

En el área de Denegación de servicio distribuido (DDoS), la inundación de TCP SYN fue uno de los primeros vectores de ataque que se encontró, y ha permanecido significativa incluso ahora, casi 20 años desde su primer uso.

Un ataque DDoS de inundación de TCP SYN genera y envía una gran cantidad de paquetes TCP [SYN] a un servidor de destino en un intento de hacer que el servidor genere múltiples paquetes TCP [SYN-ACK], pero no envía el último paquete TCP [ACK], lo que resulta en múltiples conexiones abiertas. Agotando los recursos de conexión abiertos del servidor se pueden negar sus servicios.

Los ataques más efectivos son causados por direcciones IP de origen falsificadas al azar que se dirigen a un servicio TCP específico.

Por otro lado, el escaneo de puertos generalmente consiste en numerosas conexiones, que tienen diferentes puertos de destino para cada conexión y/o tráfico (no es un protocolo de enlace TCP completo, paquetes UDP dirigidos a puertos aleatorios, etc).

Esencialmente, el comportamiento es similar a un ataque DDoS, aparte del hecho de que la fuente del tráfico es conocida y está dentro de la red.

Es probable que dicho tráfico provoque un alto consumo de CPU en Check Point *Security Gateway/Quantum Spark*:

- Conexiones TCP: debido a que *SecureXL* no puede acelerar las conexiones, ya que constantemente aleatoriza el puerto TCP de destino.
- Conexiones UDP: debido a la gran cantidad de conexión UDP que se dirige cada vez a un puerto diferente.

A continuación se incluyen algunas configuraciones recomendadas para reforzar Check Point *Security Gateway/Quantum Spark* contra este tipo de tráfico:

Habilitar y configurar ***Multi-Queue***: Una inundación de TCP SYN generalmente llega solo a una tarjeta de interfaz de red externa. La función de *Multi-Queue* mejora el rendimiento de *Security Gateway/Quantum Spark* durante los ataques de inundación de TCP SYN mediante la configuración de más de una cola de tráfico para cada tarjeta de interfaz de red y el uso de más núcleos de CPU para la aceleración del tráfico. Se debe ejecutar en máquinas con 2 o más

núcleos de CPU. Para ello, entrar como EXPERT y ejecutar los comandos siguientes: *cpmq set* y poner en ON las interfaces correspondientes. Para verificar que todo está correcto: *cpmq get –v.*

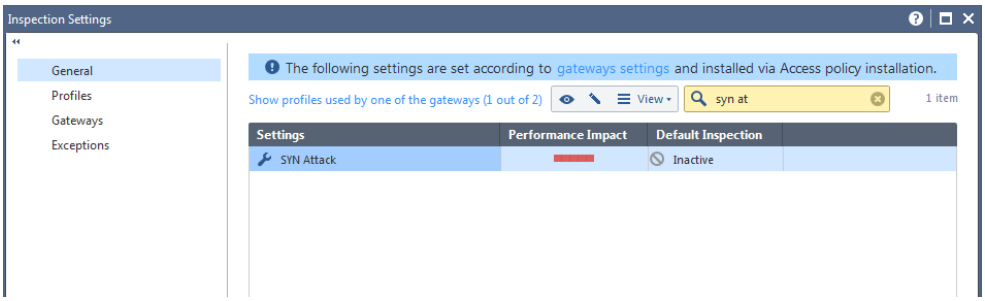
Utilizar **interfaces de *bonding***: configure la agregación de enlaces con el modo de compartir carga (activo/activo, Load Sharing) en la interfaz del *Security Gateway/Quantum Spark* para aumentar el ancho de banda disponible.

Active la **protección IPS 'SYN Attack' (SYNDefender)** y configúrela para que funcione en el modo 'SYN Cookie'. Cuando se habilita "SYN Cookie mode" se envía un paquete TCP [SYN-ACK] con un número de secuencia que le permite al *Security Gateway/Quantum Spark* verificar que el cliente es legítimo al recibir el paquete TCP [ACK]. El número de secuencia incluye un *hashing* de las direcciones IP, ambos puertos, etc. Por lo tanto:

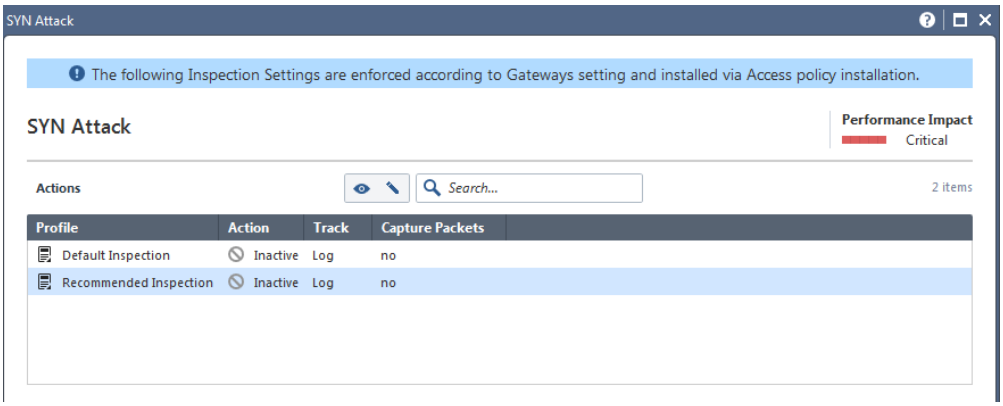
- La conexión TCP no se guarda en la tabla conexiones hasta que se verifique que la conexión es legítima.
- La conexión TCP no pasa a través de la Base de reglas hasta que se verifique como legítima.
- Se utiliza menos memoria en el Security Gateway/*Quantum Spark* para procesar conexiones TCP.

Para activarlos se debe seguir el siguiente procedimiento:

- En la barra de herramientas de navegación ir a : MANAGE & SETTINGS ➔ Blades.
- En la sección “General”, pulse en: “Inspection Settings”.
- En el árbol de la izquierda, seleccione “General” y busque “SYN Attack”.

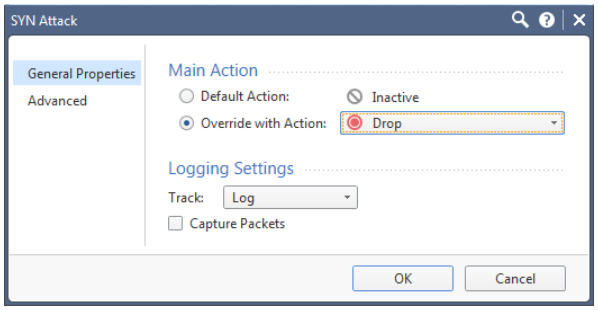


- Pulsar con el botón derecho en la protección y seleccione Editar.

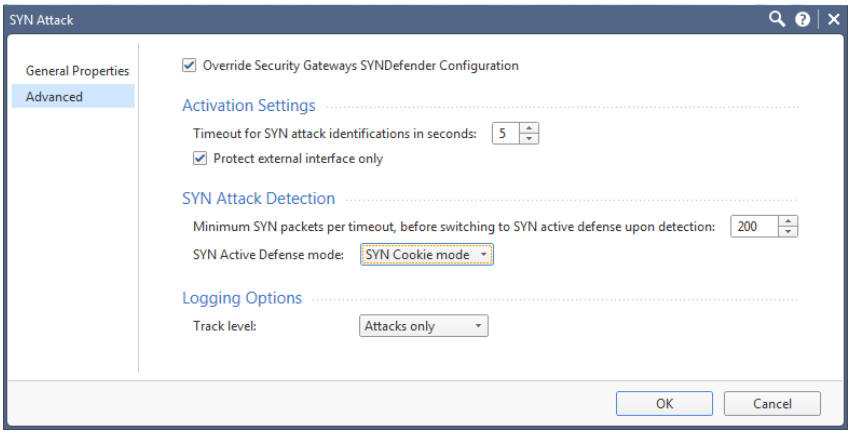


- Seleccionar el perfil IPS relevante pulsando en el botón Editar (lápiz).

– En el árbol de la izquierda, pulse en “Propiedades generales” y seleccione “Override with Action”. Seleccionar “Drop”.



– En el árbol de la izquierda, pulse en “Advanced” y configure los siguientes valores, pulse en Aceptar:



En el *Security Gateway/Quantum Spark*, configure manualmente la protección IPS 'SYN Attack' (SYNDefender) para que funcione en el modo SYN Cookie. Para ello establezca manualmente el valor del parámetro del kernel *asm_synatk_mode en 2*.

Para verificar el valor actual de este parámetro del kernel:

```
fw ctl get int asm_synatk_mode.
```

Para establecer el valor deseado para este parámetro de kernel sobre la marcha (no sobrevive al reinicio):

```
fw ctl set int asm_synatk_mode 2.
```

Para establecer el valor deseado para este parámetro de kernel de forma permanente:

– Crear el archivo fwkern.conf (si aún no sale):

```
Expert @ HostName] # touch $ FWDIR / boot / modules / fwkern.conf
```

– Editar el fwkern.conf en el editor de Vi:

```
[Expert @ HostName] # vi $ FWDIR / boot / modules / fwkern.conf
Agregar la siguiente línea (no se permiten espacios ni comentarios):
asm_synatk_mode = 2
```

– Guardar los cambios y salga del editor Vi.

– Verificar el contenido del archivofwkern.conf:

```
[Expert @ HostName] # cat $ FWDIR / boot / modules / fwkern.conf
```

- Reiniciar el Security Gateway/*Quantum Spark*.
- Verificar que se haya establecido el nuevo valor:

```
[Expert @ HostName] # fw ctl get int asm_synatk_mode
```

- Instalar la política de acceso en Security Gateway/*Quantum Spark*.

Active y configure la protección **IPS 'Aggressive Aging'** que ayuda a administrar la capacidad de la tabla de conexiones y el consumo de memoria del cortafuegos. Además, introduce un nuevo conjunto de "short timeouts" llamados "Aggressive timeouts". Cuando una conexión está inactiva por más de su "aggressive timeout", se marca como elegible para eliminación. Cuando la tabla de Conexiones de *Security Gateway/Quantum Spark* o el consumo de memoria alcanza el umbral definido por el usuario, *Aggressive Aging* comienza a eliminar las conexiones "elegibles para ser eliminadas", hasta que el consumo de memoria o la capacidad de las conexiones disminuyan al nivel deseado.

Esta configuración permite que la máquina *Security Gateway/Quantum Spark* maneje grandes cantidades de tráfico inesperado, especialmente durante un ataque de denegación de servicio.

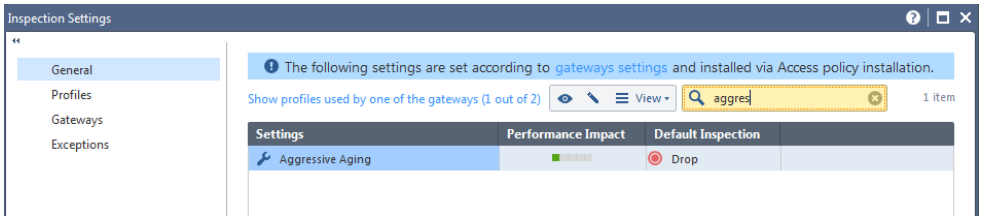
Si se excede el umbral definido, cada conexión entrante desencadena la eliminación de diez conexiones de la lista elegible para eliminación hasta que el consumo de memoria o la capacidad de las conexiones caiga por debajo del límite de cumplimiento. Si no hay conexiones elegibles para eliminación, no se eliminan conexiones en ese momento, pero la lista se verifica después de cada conexión subsiguiente que exceda el umbral.

Las configuraciones de "timeouts" son un factor clave en la configuración del consumo de memoria. Cuando los "timeouts" son bajos, las conexiones se eliminan más rápido de la tabla de conexiones del *Security Gateway/Quantum Spark*, lo que permite que maneje más conexiones simultáneamente. Cuando el consumo de memoria excede su umbral, es mejor trabajar con "timeouts" más cortos que puedan mantener la conectividad de la gran mayoría del tráfico.

El principal beneficio del "Aggressive Aging" es que comienza a funcionar cuando la máquina todavía tiene memoria disponible y la tabla de conexiones no está completamente llena. De esta manera, reduce las posibilidades de problemas de conectividad que podrían haber ocurrido en condiciones de bajos recursos.

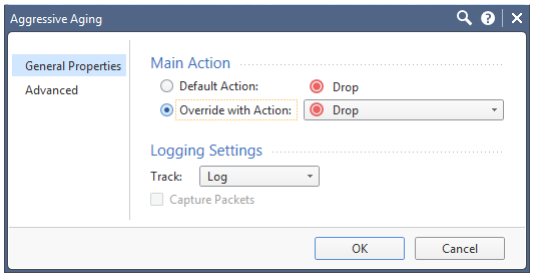
Para su configuración se debe seguir el siguiente procedimiento:

- En herramientas de navegación, pulsar: *MANAGE & SETTINGS* ➔ *Blades.*
- En la sección "General", seleccione: "Inspection Settings".
- En el árbol de la izquierda, pulse en "General" y buscar "Aggressive Agging".

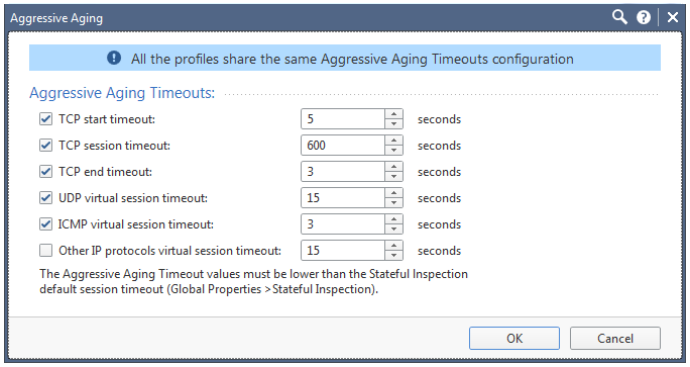


- Pulsar con el botón derecho en la protección y seleccione "Editar".

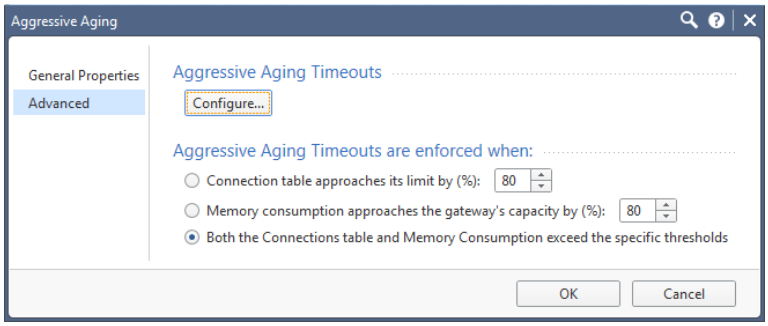
- Seleccionar el perfil IPS relevante: pulse en el botón Editar (lápiz).
- En el árbol de la izquierda, pulse en "Propiedades generales" y seleccione "Override with Action". Seleccionar "Drop".



- En el árbol de la izquierda, haga clic en "Advanced" y en "Configurar". Configurar los siguientes valores y pulse en Aceptar:



- Configurar el umbral deseado para hacer cumplir los tiempos de espera de envejecimiento agresivo.



- Pulsar en Aceptar para cerrar la ventana de propiedades y en el botón Cerrar.
- Instalar la política de acceso en *Security Gateway/Quantum Spark*.

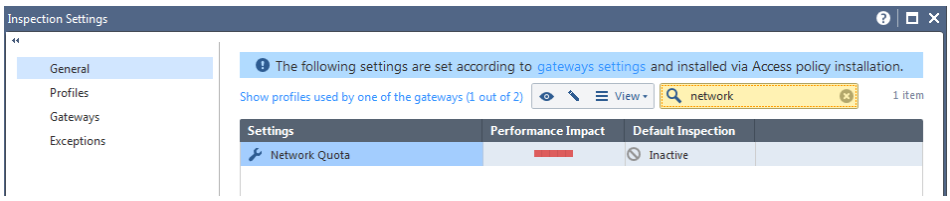
Active y configure la protección **IPS "Network Quota"** para limitar el número de conexiones por dirección IP. Cuando el número de conexiones de un determinado host supera el límite configurado, se bloquean todas las conexiones nuevas desde esa dirección IP de origen.

Puede establecer excepciones para esta protección IPS por dirección IP de origen o *Security Gateway/Quantum Spark*.

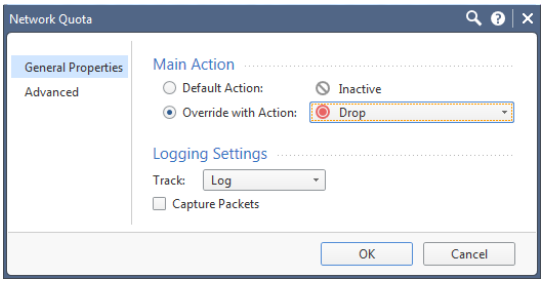
El procedimiento a seguir para su configuración:

- En la barra de herramientas de navegación, haga clic en: *MANAGE & SETTINGS* ➔ *Blades.*

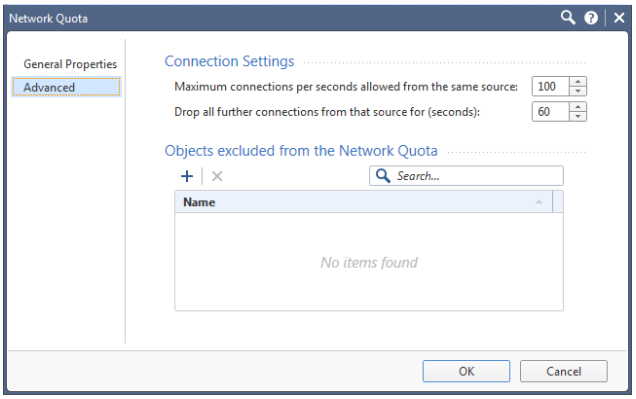
- En la sección “General”, pulse en “Inspection Settings”.
- En el árbol de la izquierda, pulse en “General” y buscar “Network Quota”.



- Pulsar con el botón derecho en la protección y seleccione Editar.
- Seleccionar el perfil IPS relevante: pulse en el botón Editar.
- En el árbol de la izquierda, pulse en Propiedades generales y seleccione “Override with Action”. Seleccionar “Drop”.



- En el árbol de la izquierda, en “Advanced”, establezca el tiempo de espera deseado y agregue el objeto de aplicación/host específico a excluir:

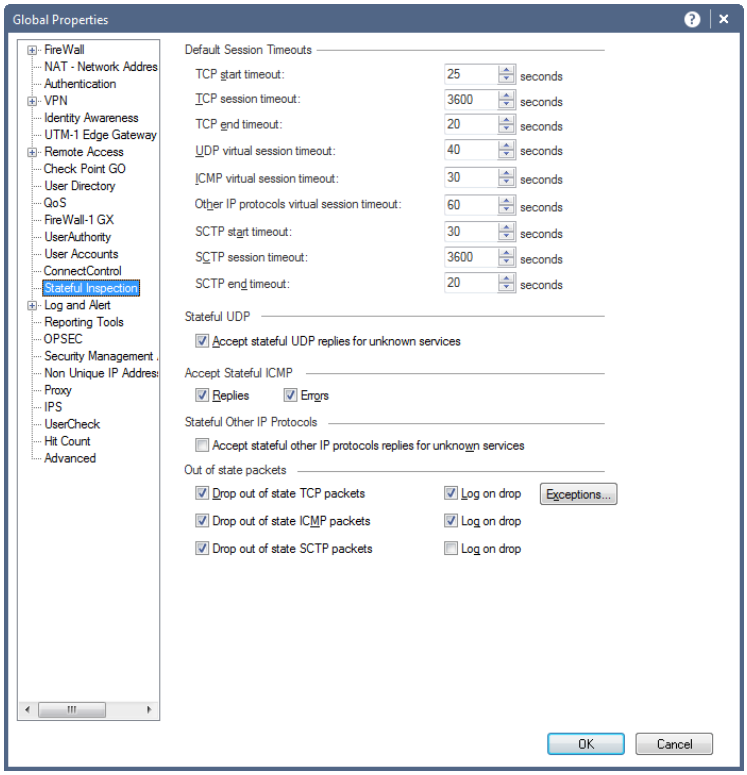


- Pulsar en Aceptar para cerrar la ventana de propiedades "network Quota" y en el botón "Cerrar".
- Instalar la política de acceso / seguridad de red en *Security Gateway/Quantum Spark*.

Notas: cuando la Cuota de red está habilitada, las *Plantillas SecureXL* se deshabilitan automáticamente. Se muestra una advertencia al respecto cuando se instala la política. Sólo se bloquean las nuevas conexiones, las existentes no.

Ajuste stateful **inspection timeouts para TCP and UDP**. La reducción de los valores de tiempo de espera de TCP y UDP globales puede ayudar a evitar que la tabla de conexiones del kernel se llene durante un ataque DoS. El procedimiento a seguir es:

- Abrir propiedades globales.
- Vaya al panel de “stateful inspection”.



Configuraciones recomendadas:

Setting	Recommended value
TCP start timeout	2-5
UDP virtual session timeout	2-5

Nota: la reducción de este tiempo de espera podría afectar al tráfico, especialmente para los usuarios que están muy alejados geográficamente de los centros de datos. Por lo tanto, es importante monitorizar el entorno mientras se cambian estas configuraciones.

Configurar **reglas "Rate Limiting**" para mitigación DoS (*fw samp*). "Rate Limiting" es una defensa contra los ataques DoS. Una política basada en reglas que limita el tráfico que proviene de fuentes específicas y utiliza servicios específicos. "Rate Limiting" es impuesta por SecureXL en:

- Ancho de banda y tasa de paquetes.
- Número de conexiones concurrentes.
- Tasa de conexión.

Para añadir una nueva regla de "Rate Limiting":

```
[Expert@HostName:0]# fw samp add [-t <timeout>] {[-a <d|n|b>]} [-l <r
|a>] [-n <name>] [-c <comment>] [-o <originator>] quota <quota limits>
```

-t: período de tiempo (en segundos), durante el cual se aplicará la política.

-a <d | n | b >: especifica la acción: d (Drop), n (Notify) y b (Bypass).

-l <r | a>: especifica el tipo de log: r (Rgular Log) y a (Alert).

-n <name>: nobre para la regla.

-c <comment>: comentario para la regla.

-o <originator>: especifica quién origina esta regla.

quota <quota limits>: especifica que se debe agregar con argumentos de filtro.

Ejemplos:

```
# fw samp add -a d -l r quota service 6/22-30 source cidr:192.168.2.202/32 pkt-rate 1 flush true
```

Para ver las reglas *fw samp* existentes:

```
fw samp get
fw samp get -l
```

Por ejemplo:

```
[Expert@edale-r1:0]# fw samp get
operation=add uid=<5b858f48,00000000,0b5016ac,0000298f> target=all
timeout=indefinite action=drop log=log service=6/22 source=cidr:192.168.1.202/32
pkt-rate=1 flush=true req_type=quota
operation=add uid=<5b858f1c,00000000,0b5016ac,00002929> target=all
timeout=indefinite action=drop log=log service=6/22 source=cidr:192.168.2.202/32
pkt-rate=1 flush=true req_type=quota
operation=add uid=<5b858f20,00000000,0b5016ac,00002939> target=all
timeout=indefinite action=drop log=log service=6/22 source=cidr:192.168.4.202/32
pkt-rate=1 flush=true req_type=quota
```

Bloquee el tráfico proveniente de **direcciones IP maliciosas conocidas**. *SecureXL* permite bloquear el tráfico proveniente de direcciones IP maliciosas conocidas:

- Basado en la lista de direcciones IP maliciosas conocidas.
- Basado en la lista de nodos de TOR conocidos.

Por ejemplo, Check Point mantiene una lista de direcciones IP conocidas como Nodos de salida de TOR. *Security Gateway/Quantum Spark* consulta la “Check Point's Threat Cloud “ y bloquea todo el tráfico de estas direcciones IP de origen (Check Point actualiza estas listas periódicamente): https://secureupdates.checkpoint.com/IP-list/TOR.txt

También se puede bloquear las direcciones IP proporcionadas por fuentes de información con actualizaciones automáticas. *Security Gateway/Quantum Spark* descargará y actualizará los” feeds” cada 20 minutos. Se enviará un registro de control al actualizar las reglas.

Al bloquear una dirección IP de la fuente, se mostrará un registro en *SmartLog* con el campo "Acción" que dice Descartar y con el campo "Información" que dice "Mensaje SecureXL: Infracción de cuota".

El procedimiento a seguir en el servidor de administración es:

- Prepare un archivo de texto sin formato que contenga una lista de *Security Gateways/Quantum Sparks* que deben realizar esta aplicación (indicada a continuación como *<gw_list_file>):*
    - Cada línea debe contener nombre o dirección IP del *Security Gateway/Quantum Spark.*

- Para comentarios, use el carácter # al principio de una línea.

– Prepare un archivo de texto sin formato que contenga una lista de URL (fuentes), desde donde los Security Gateways/*Quantum Sparks* descargarán las direcciones IP que deberían estar bloqueadas, por ejemplo, https://secureupdates.checkpoint.com/IP-list/TOR .txt (este archivo se indica a continuación como *<feed_file>):*

- Cada línea debe contener una sola URL completa.
- Para comentarios, use el carácter # al principio de una línea.

Notas: Las fuentes de información IP deben contener una dirección IP (IPv4 o IPv6), o un rango (por ejemplo, 172.23.42.2-172.23.42.15) por línea.

– Opcionalmente se puede preparar un archivo de texto sin formato que contenga una lista de direcciones IP (en el formato de fuente de información IP mencionado anteriormente) que debe omitir (se indica a continuación como *<bypass_file>).* Incluso si las fuentes personalizadas contienen esas direcciones IP, serán excluidas.

– Descargue estos scripts de shell (*ip_block_sk103154.tar*):

https://supportcenter.checkpoint.com/supportcenter/portal/role/supportcenterUser/page/default.psml/media-type/html?action=portlets.DCFileAction&eventSubmit_doGetdcdetails=&fileid=56231

– Transfiera estos scripts de shell al Servidor de administración (en algún directorio, por ejemplo, */ some_path_to_scripts /).*

– Conéctese a la línea de comandos en el servidor de administración e inicie sesión en el modo Experto.

– Descomprima los scripts de shell y asigne permisos de ejecución:

```
[Expert@HostName:0]# cd /some_path_to_scripts/
[Expert@HostName:0]# tar -xvf ip_block_sk103154.tar
[Expert@HostName:0]# chmod -v u+x ip_block*
```

– Use el script ip_block_activate.sh para gestionar los Security Gateways/*Quantum Sparks*:

[Expert@HostName:0]# ./ip_block_activate.sh -a <on|off|stat|allow> [-g <gw_list_file>] [-b <bypass_file>] [-f <feed_file>] [-s /full_path_to/ip_block.sh]

Nota importante: Al ejecutar el script ip_block_activate.sh por primera vez, también debe usar el argumento "-s /full_path_to/ip_block.sh".

Por ejemplo, habilitar la funcionalidad:

```
[Expert@HostName:0]# ip_block_activate.sh -a on -g gw_list.txt -f feeds_list.txt
[-s /full_path_to/ip_block.sh]
```

Deshabilitar la funcionalidad:

```
[Expert@HostName:0]# ip_block_activate.sh -a off -g gw_list.txt
```

Para bloquear el trafico desde nodos TOR conocidos, la base de datos de alimentación de Check Point https://secureupdates.checkpoint.com/IP-list/TOR.txt es solo una base “best-effort”. Para bloquear completamente el acceso, *Appliaction Control* y HTTPS Inspection deben estar habilitadas en el *Gateway*.

El procedimiento a seguir es:

- Crear una copia del script actual de *$ CPDIR / bin / IP-blacklist.sh*:

```
[Expert@HostName:0]# cp -v $CPDIR/bin/IP-blacklist.sh $CPDIR/bin/IP-blacklist-TOR.sh
```

- Modificar los valores predeterminados en $ CPDIR / bin / IP-blacklist-TOR.sh:

```
[Expert@HostName:0]# vi $CPDIR/bin/IP-blacklist-TOR.sh
```

- Modificar línea #3

from:	url="https://secureupdates.checkpoint.com/IP-list/IP-blacklist.txt"
to:	url="https://secureupdates.checkpoint.com/IP-list/TOR.txt"

- Modificar línea #4

from:	comment="threatcloud_ip_block"
to:	comment="threatcloud_TOR_block"

- Salvar los cambios y salga del editor Vi.
- Crear una copia del script actual de $ CPDIR / bin / ip_block.sh:

```
[Expert@HostName:0]# cp -v $CPDIR/bin/ip_block.sh $CPDIR/bin/ip_block_TOR.sh
```

- Modificar los valores predeterminados $ CPDIR / bin / ip_block_TOR.sh:
- Editar el script $ CPDIR / bin / ip_block_TOR.sh:

```
[Expert@HostName:0]# vi $CPDIR/bin/ip_block_TOR.sh
```

- Modificar línea #15

from:	echo "$(date): Starting" >> $FWDIR/log/ip_block.log
to:	echo "$(date): Starting" >> $FWDIR/log/ip_block_TOR.log

- Modificar línea #19

from:	$CPDIR/bin/cpd_sched_config add ip_block -c "$CPDIR/bin/IP-blacklist.sh" -e 1200 -r -s
to:	$CPDIR/bin/cpd_sched_config add ip_block_TOR -c "$CPDIR/bin/IP-blacklist-TOR.sh" -e 1200 -r -s

- Modificar línea #20

from:	echo "ip_block: Known malicious IP blocking mechanism is ON"
to:	echo "ip_block_TOR: Known TOR Exit Nodes blocking mechanism is ON"

- Modificar línea #24

from:	$CPDIR/bin/cpd_sched_config delete ip_block -r
to:	$CPDIR/bin/cpd_sched_config delete ip_block_TOR -r

- Modificar línea #26

from:	echo "ip_block: Known malicious IP blocking mechanism is OFF"
to:	echo "ip_block_TOR: Known TOR Exit Nodes blocking mechanism is OFF"

- Modificar línea #30

from:	cpd_sched_config print | awk 'BEGIN{res="OFF"}/Task/{flag=0}/ip_block/{flag=1}/Active: true/{if(flag)res="ON"}END{print "ip_block: Known malicious IP blocking mechanism status is "res}'
to:	cpd_sched_config print | awk 'BEGIN{res="OFF"}/Task/{flag=0}/ip_block_TOR/{flag=1}/Active: true/{if(flag)res="ON"}END{print "ip_block_TOR: Known TOR Exit Nodes blocking mechanism status is "res}'

– Modificar línea #34-39

from:	echo 'Usage:' echo ' ip_block.sh <option>' echo 'Option:' echo ' on: blocks malicious IPs' echo ' off: stops malicious IPs blocking' echo ' stat: prints the status of malicious IP blocking'
to:	echo 'Usage:' echo ' ip_block_TOR.sh <option>' echo 'Option:' echo ' on: blocks Known TOR Exit Nodes' echo ' off: stops Known TOR Exit Nodes blocking' echo ' stat: prints the status of Known TOR Exit Nodes blocking'

– Modificar línea #40

from:	echo "ip_block: This utility is supported on GAIA Security Gateway only"
to:	echo "ip_block_TOR: This utility is supported on GAIA Security Gateway only"

– Guardar los cambios y salga de Vi editor.

– Ejecutar manualmente este script:

```
[Expert@HostName:0]# ip_block_TOR.sh { on | off | stat}
```

7.5 NETWORK ADDRESS TRANSLATION (NAT)

La traducción de direcciones de red (NAT) permite a los administradores de seguridad superar las limitaciones de direccionamiento IP, lo que permite la asignación de direcciones IP privadas y esquemas de direcciones internas no registradas.

Se emplea NAT por una variedad de razones, que incluyen:

– Para direcciones IP privadas utilizadas en redes internas.

– Para limitar el acceso a la red externa.

– Para facilidad y hacer más flexible la administración de red.

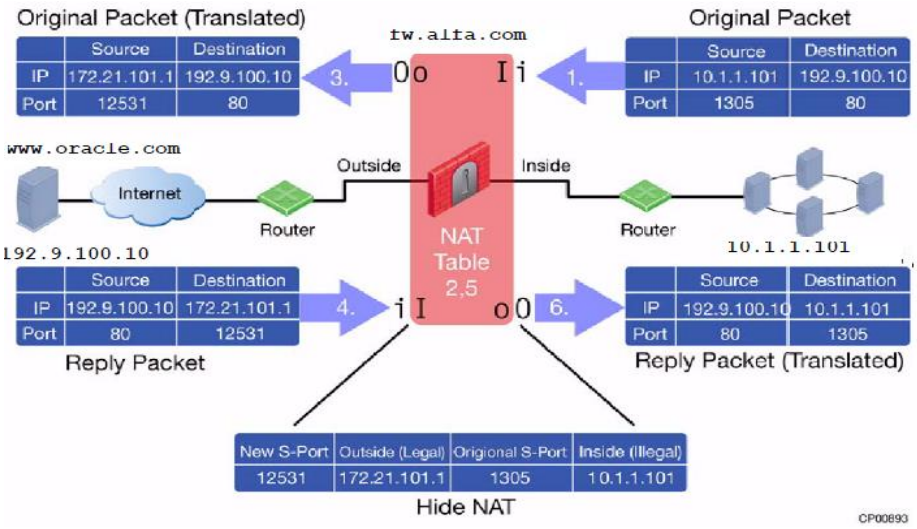
Security Gateway/Quantum Spark admite dos (2) tipos de NAT:

– *Hide NAT:* relación de muchos a uno, donde múltiples computadoras están representadas por una dirección única. Conocido como NAT dinámico.

– *Static NAT*: una relación uno a uno donde cada host se traduce a una dirección única; esto permite que las conexiones se inicien interna y externamente. Un ejemplo sería un servidor web o un servidor de correo que necesita permitir conexiones iniciadas externamente.

NAT se puede configurar en *hosts*, nodos, redes, rangos de direcciones y objetos dinámicos de Check Point. Se puede configurar automáticamente o creando reglas de NAT manuales. Las

reglas de NAT manuales ofrecen flexibilidad porque pueden permitir la traducción tanto del origen, como del destino del paquete y permiten la traducción de servicios.



Hide Address es la dirección detrás de la cual se oculta la red, el rango de direcciones o el nodo. Es posible ocultarse detrás de la interfaz del *Gateway* o de una dirección IP específica. Elegir una dirección IP pública fija es una opción si desea ocultar la dirección de *Security Gateway/Quantum Spark*, sin embargo, esto supone usar una dirección IP enrutable públicamente.

El método predeterminado para el NAT de destino es "del lado del usuario", donde el NAT ocurre en la interfaz de entrada más cercana al usuario. Supongamos que el usuario está fuera del *Security Gateway/Quantum Spark* y el servidor está dentro del *Security Gateway/Quantum Spark* con la configuración automática de *static NAT*.

Cuando el usuario inicia una conexión para acceder a la dirección IP NAT del servidor, sucede lo siguiente con el paquete original en un NAT del lado del usuario:

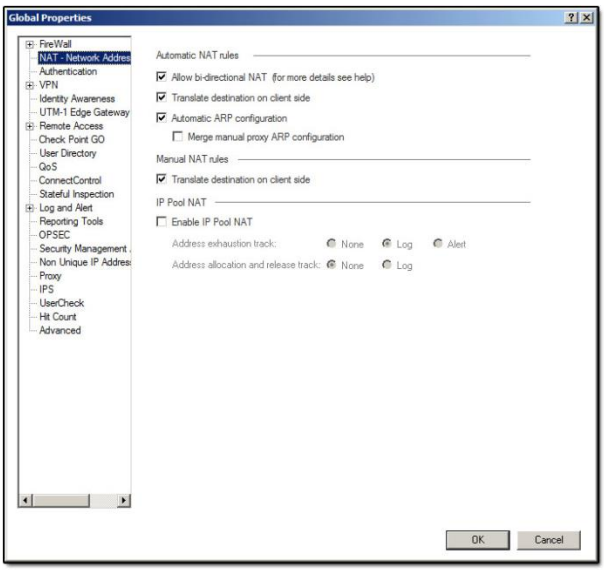
Paquete Origen: el paquete llega a la interfaz de entrada, pre-inbound 'i', destinado para el servidor web y pasa la Política de seguridad y las reglas de NAT. Si se acepta, la información del paquete se agrega a la tabla de conexiones y el destino se traduce en el lado posterior a la entrada de la interfaz, post-Inbound 'I', antes de enrutarse.

El paquete llega a la pila TCP/IP del *Security Gateway/Quantum Spark* y se enruta a la interfaz de salida, pre-outbound 'o'. El paquete se reenvía a través del *kernel*, interfaz post-Outbound 'O', y se enruta al servidor web.

Paquete Respuesta: el servidor web responde y hace *hit* de la interfaz de entrada, pre-indbound 'i', del *Security Gateway/Quantum Spark*.

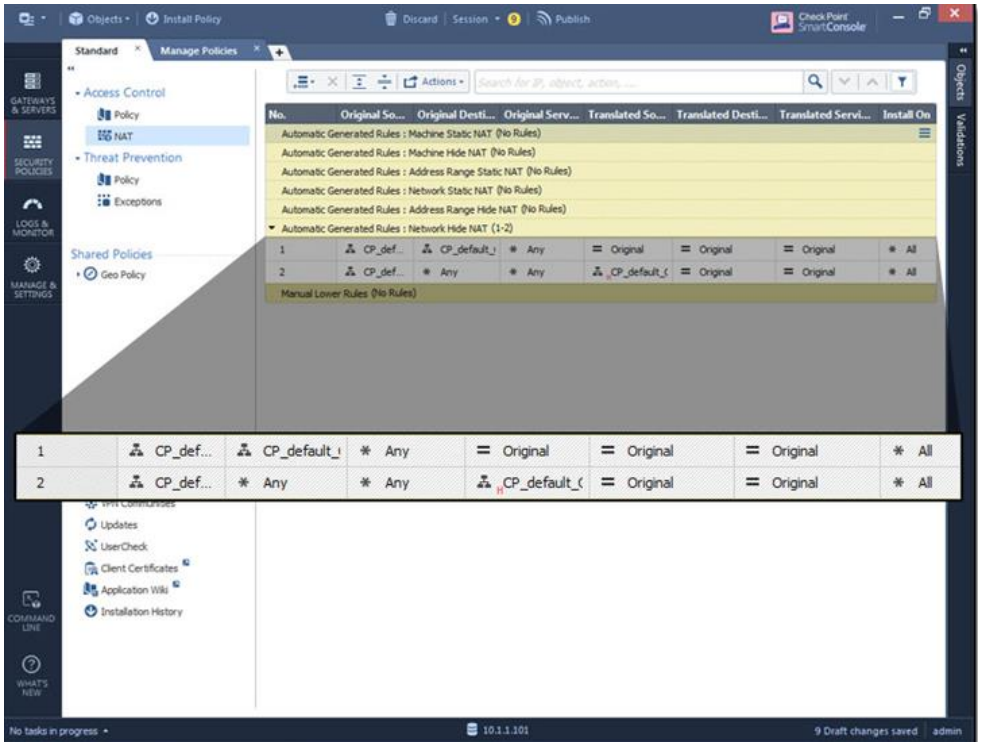
El paquete pasa el filtro de la política ya que se encuentra en la tabla de conexiones y llega al lado post-inbound 'I' del Kernel. En la pila TCP/IP del *Security Gateway/Quantum Spark* se enruta a la interfaz de salida pre-outbound 'o'.

El paquete pasa por la interfaz de salida y se traduce a la dirección IP estática del NAT cuando sale del *Security Gateway/Quantum Spark* de seguridad, post-Outbound 'O'. El puerto de origen no cambia.



En la mayoría de los casos, el *Security Gateway/Quantum Spark* crea automáticamente reglas de NAT basadas en la información derivada de las propiedades del objeto. Las siguientes propiedades globales se pueden modificar para ajustar el comportamiento de las reglas de NAT automáticas a nivel global:

- *Allow bi-directional* NAT: verificará todas las reglas de NAT para ver si hay una coincidencia de origen en una regla y una coincidencia de destino en otra regla. El *Security Gateway/Quantum Spark* utilizará las primeras coincidencias encontradas y aplicará ambas reglas al mismo tiempo. Si no se selecciona, solo se aplicará la primera coincidencia.
- *Translate Destination on client side*: Si no se selecciona, se requiere una ruta de *host* en el *Security Gateway/Quantum Spark* para enrutar al servidor de destino.
- *Automatic ARP configuration*: La configuración ARP automática agrega las entradas ARP necesarias para lograr esta tarea. Esta propiedad se aplica solo a las reglas de NAT creadas automáticamente.
- *Merge manual proxy ARP*: se debe seleccionar esta opción para fusionar configuraciones ARP automáticas y manuales. La configuración ARP de proxy manual es necesaria para las reglas NAT estáticas manuales. ARP se puede configurar a través del portal Gaia o Clish.



Las reglas de NAT se dividen en dos elementos: paquete original y paquete traducido. Los elementos de la sección Paquete Original informan a un *Security Gateway/Quantum Spark* qué paquetes coinciden con la regla.

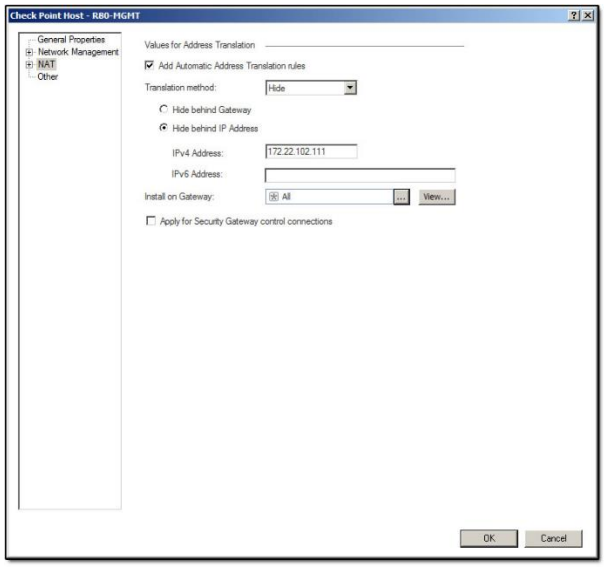
Los elementos del Paquete Traducido definen cómo el *Security Gateway/Quantum Spark* debe modificar el paquete. La configuración del objeto de red crea dos reglas en la política de Traducción de direcciones.

La primera regla evita la traducción de paquetes que viajan desde el objeto traducido a sí mismo. La segunda regla ordena a *Security Gateway/Quantum Spark* que traduzca paquetes cuya dirección IP de origen sea parte de la red. Esta regla traduce paquetes de direcciones privadas a la dirección IP de la interfaz de salida de *Security Gateway/Quantum Spark*.

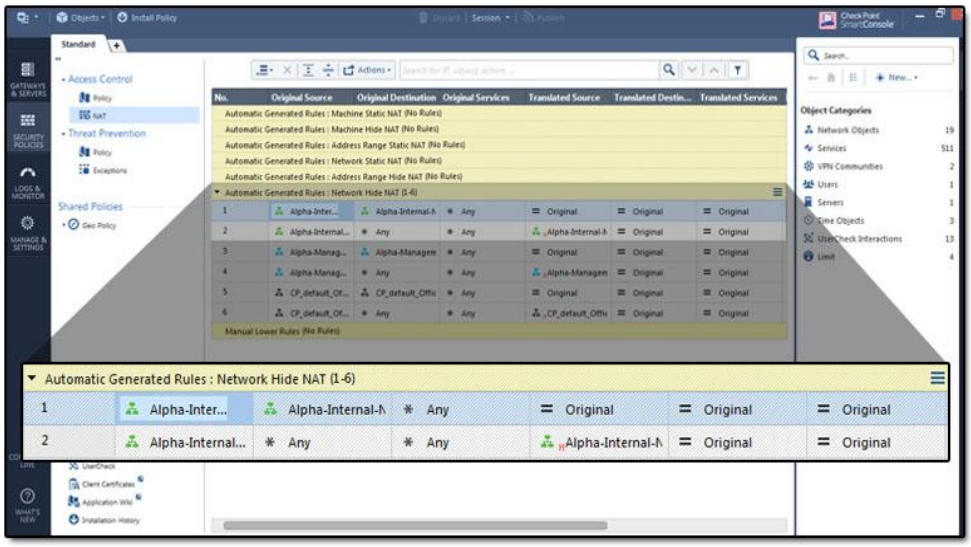
Como *Hide NAT* también modifica los puertos de origen, no es necesario agregar otra regla para los paquetes de respuesta. La información registrada en las tablas de estado de *Security Gateway/Quantum Spark* se usará para modificar la dirección IP de destino y el puerto de destino de los paquetes de respuesta.

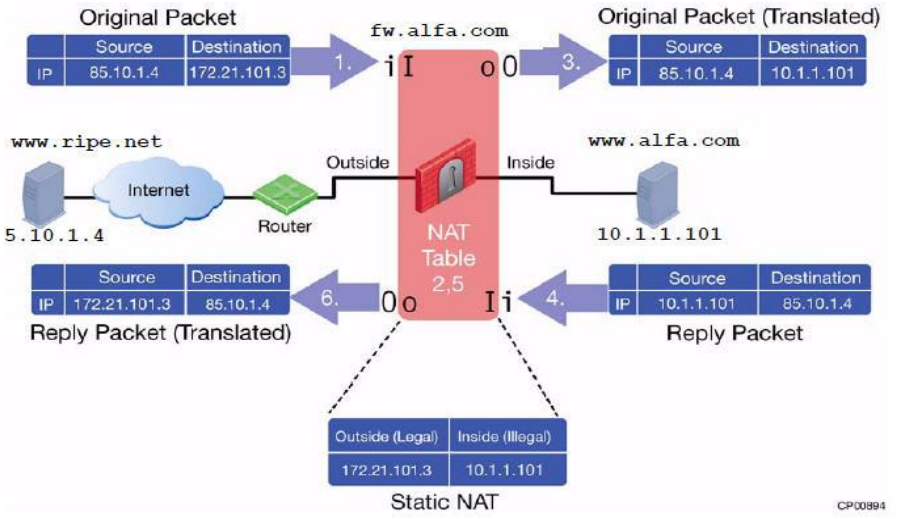
El uso de otra dirección IP accesible externamente para *Hide NAT* se considera la mejor práctica. La siguiente figura ilustra cómo configurar las propiedades de NAT para una red que usará otra dirección IP accesible externamente cuando se traduce dinámicamente.

Para la creación automática de reglas NAT, *Security Gateway/Quantum Spark* realiza todas las entradas necesarias de la ruta y la tabla ARP y procesará los paquetes destinados para *HR_Server* aunque esa dirección IP no esté vinculada a su interfaz. La dirección seleccionada para ocultar las redes internas debe estar en la misma subred que la dirección IP de la interfaz a la que llegarán los paquetes.



Al igual que el *Hide NAT* detrás de una dirección IP del *Security Gateway/Quantum Spark*, la configuración con otra dirección IP accesible externamente también crea dos reglas. La primera regla ordena al *Security Gateway/Quantum Spark* que no traduzca el tráfico cuyo origen y destino es el objeto para el que se configura *Hide NAT*. La segunda regla traduce la dirección de origen de los paquetes no destinados para el objeto para el que se configura *Hide NAT*.





Aplicamos *Static NAT* a un servidor al que se debe acceder directamente desde fuera del *Security Gateway/Quantum Spark*. El paquete generalmente se inicia desde un *host* fuera del cortafuegos. Cuando el usuario inicia el tráfico a la dirección *Static NAT*, el destino del paquete se traduce.

La configuración para realizar *Static NAT* a un host es similar a la configuración de un *Security Gateway/Quantum Spark* para realizar *Hide NAT* utilizando otra dirección IP accesible externamente.

Para que el enrutamiento funcione correctamente, la configuración a traducir una dirección IP debe estar en la misma subred que la dirección IP del *Security Gateway/Quantum Spark*. Cuando se utiliza la creación automática de reglas NAT, se realizan los ajustes necesarios en la configuración ARP.

La configuración de un objeto para la creación automática de reglas Static NAT agrega dos reglas a la política de Traducción de direcciones. Para *Static NAT*, ambas reglas son reglas de traducción. En el ejemplo anterior, *Security Gateway/Quantum Spark* cambia la dirección de origen de una dirección privada a la dirección pública.

7.6 ENRUTAMIENTO

Para poder enrutar tráfico IP es necesario que el cortafuegos disponga de la información de las redes alcanzables. Los comandos para editar esta información a través de la consola e introducir rutas estáticas tipo agujero negro, desactivar o activar rutas hacia destinos concretos, rechazar tráfico o desactivar todas las rutas de una red concreta son los siguientes:

```
set static-route VALUE nexthop blackhole
set static-route VALUE nexthop gateway address VALUE off
set static-route VALUE nexthop gateway address VALUE on
set static-route VALUE nexthop reject
set static-route VALUE off
```

Donde *VALUE* es en primer lugar la red a alcanzar y posteriormente el destino a través del que se alcanza dicha red.

Para visualizar la información de enrutamiento relativa a un destino concreto *x.x.x.x* o de todos los destinos alcanzables se pueden emplear los siguientes comandos:

```
ip route show to match x.x.x.x
ip route get x.x.x.x
netstat -rn | grep x.x.x.x
netstat -rn | wc -l
cpstat os -f routing
clish -c “show route”
clish -c “show route destination  x.x.x.x “
clish -c “show configuration static-route”
```

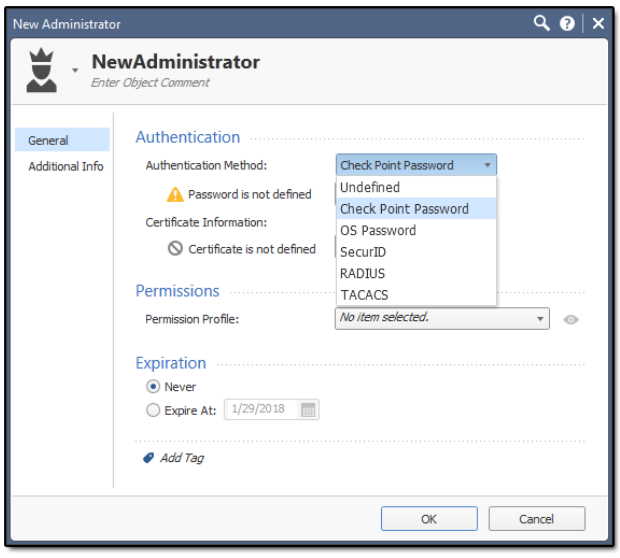
En el caso de problemas de enrutamiento se puede reiniciar el proceso correspondiente:

```
ps auxw | grep -v grep | grep -E "PID|routed" #Ver proceso corriendo
drouter stop && drouter start
drouter stop                          #Parar Demonio de Routing Dinámico
drouter start                 #Arrancar Demonio Routing Dinámico
tellpm process:routed t       #start routing process survives reboot
tellpm process:routed         #stop routing process survives reboot
```

7.7 ADMINISTRADORES Y PERFILES DE ADMINISTRACIÓN

Las cuentas de administrador se crean a través de la herramienta de configuración Check Point. Sin un método de autenticación, el administrador no puede iniciar sesión en *SmartConsole*. Las cuentas creadas a través de *SmartConsole* utilizarán uno de los siguientes esquemas de autenticación:

- Check Point Password: cada usuario definido en el *Security Management Server* tendrá una contraseña correspondiente almacenada en la base de datos local.
- OS Password: los administradores se autentican usando directorio activo, ldap, etc.
- SecurID: usa un dispositivo físico *token* o un *token* de tipo software.
- Remote Authentication Dial-In User Service (RADIUS): un servidor externo almacena credenciales de usuario y administra la autenticación de los usuarios a los dispositivos de red.
- Terminal Access Controller Access Control System (TACACS): un servidor externo almacena credenciales de usuario y administra la autenticación de los usuarios a los dispositivos de red.



Los perfiles de permisos permiten un control detallado sobre quién puede realizar ciertas tareas, como copias de seguridad, *scripts*, instalación de políticas y registro. Se puede asignar un perfil de permiso a múltiples administradores. Solo los administradores con los permisos aplicables pueden crear y administrar perfiles de permisos.

Hay tres tipos de perfil:

- Read/Write All: Pueden cambiar la configuración.
- Auditor (Read Only All): Pueden ver la configuración, pero no pueden cambiarla.
- Customized: Para configurar permisos personalizados. Para cada característica, determina si el administrador debe poder configurar la función o solo verla. Si el permiso para la característica no está seleccionado, el administrador no puede ver la característica. Si se selecciona, el administrador puede ver la característica. Junto a muchas características hay un menú desplegable con las siguientes dos opciones:
- Read: el administrador puede ver la característica pero no puede cambiar su configuración.
- Write: el administrador puede ver y cambiar la configuración de la función.

Los permisos se dividen en las siguientes pestañas:

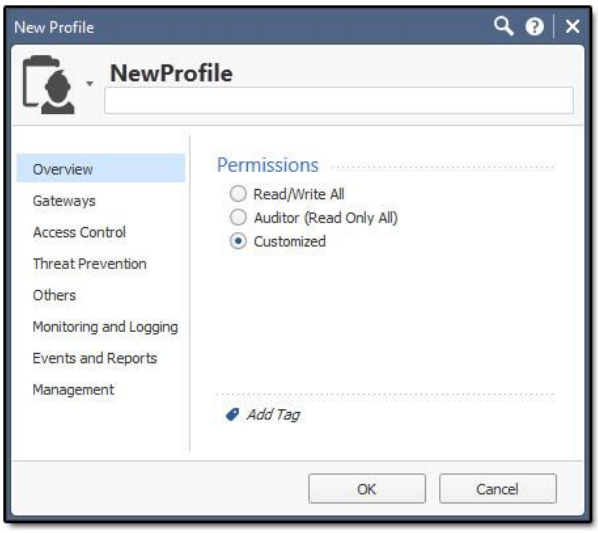
- Gateways: Los permisos de *Provisioning* y *Scripts*.
- Access Control.
- Threat Prevention.
- Others: permisos para objetos comunes, bases de datos de usuario, funciones de inspección HTTPS y certificados de cliente.
- Monitoring and Logging: Permisos para generar, ver registros y para usar funciones de monitorización.
- Events and Reports: Los permisos SmartEvent.
- Management: Permisos para administrar sesiones y administradores.

Para crear un perfil en *SmartConsole* debe ir a *Manage & Settings* ➔ *Permissions and Administrators* ➔ *Permission Profiles*. Pulsar “New Profile”. Introducir un nombre único para el perfil. Seleccionar un tipo de perfil. Pulsamos “OK”.

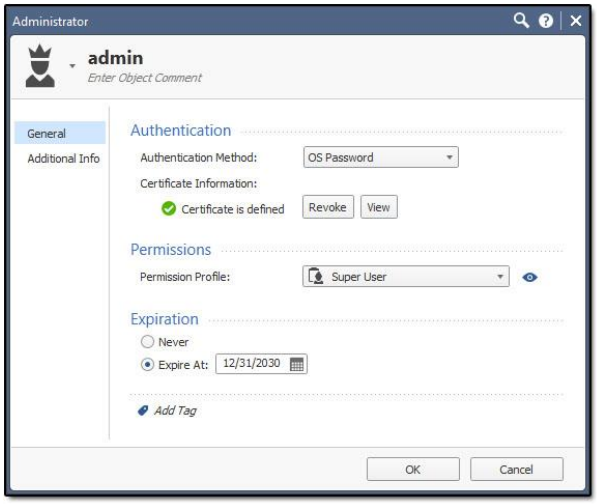
Al configurar una nueva capa en la política de Control de acceso, la pestaña “Permisos” rellenará automáticamente una lista de perfiles que tienen permisos para editar esta capa, en función de los *Blades de software* habilitados para esa capa. También se pueden agregar perfiles adicionales usando la herramienta de búsqueda.

Una cuenta de administrador puede configurarse para caducar en una fecha. Puede configurarse para mostrar las notificaciones acerca de la fecha de vencimiento al iniciar sesión. Para usar la misma configuración de vencimiento para varias cuentas, se debe cofigurar una fecha de vencimiento predeterminada.

Nota: Después de la fecha de vencimiento, la cuenta ya no está autorizada para acceder a recursos y aplicaciones de la red.



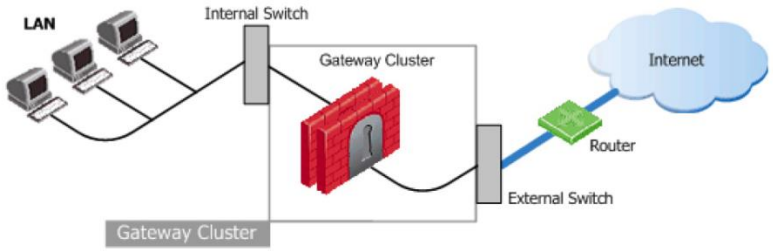
Es posible revocar un certificado de administrador. Esto permite que la cuenta de administrador continúe existiendo, pero no permite que se autentique en el *Security Management Server*. Para revocar un certificado de administrador, pulse en el botón *Revoke* en la sección "Autenticación" en la pestaña "General".



7.8 ALTA DISPONIBILIDAD

Para asegurar que los *Security Gateways/Quantum Spark* y las conexiones VPN se mantengan activas en una red corporativa, es necesario disponer de un sistema de alta disponibilidad. El fallo de una conexión de un *Security Gateway/Quantum Spark* o VPN puede provocar la pérdida de conexiones activas.

Mediante *ClusterXL* se puede proporcionar una infraestructura que no pierda datos en caso de un fallo del sistema. El *Cluster* es un grupo de *Security Gateways/Quantum Spark* idénticos y conectados que garantiza que si uno falla, otro inmediatamente toma su lugar.



ClusterXL es una solución de clúster basada en software de Check Point que proporciona redundancia del *Security Gateway/Quantum Spark* y balanceo de carga. Utiliza la sincronización de estado para mantener activas las conexiones y evitar la pérdida de datos cuando un miembro falla. Con la sincronización de estado, cada miembro conoce las conexiones que pasan por otros miembros.

ClusterXL consta de *Clusters* y miembros del *Cluster*. Un *Cluster* está formado por dos o más *Security Gateways* configurados para actuar como una unidad. Cada *Security Gateway/Quantum Spark* en un clúster *ClusterXL* es idéntico y está conectado de tal manera que si uno falla, otro inmediatamente toma su lugar.

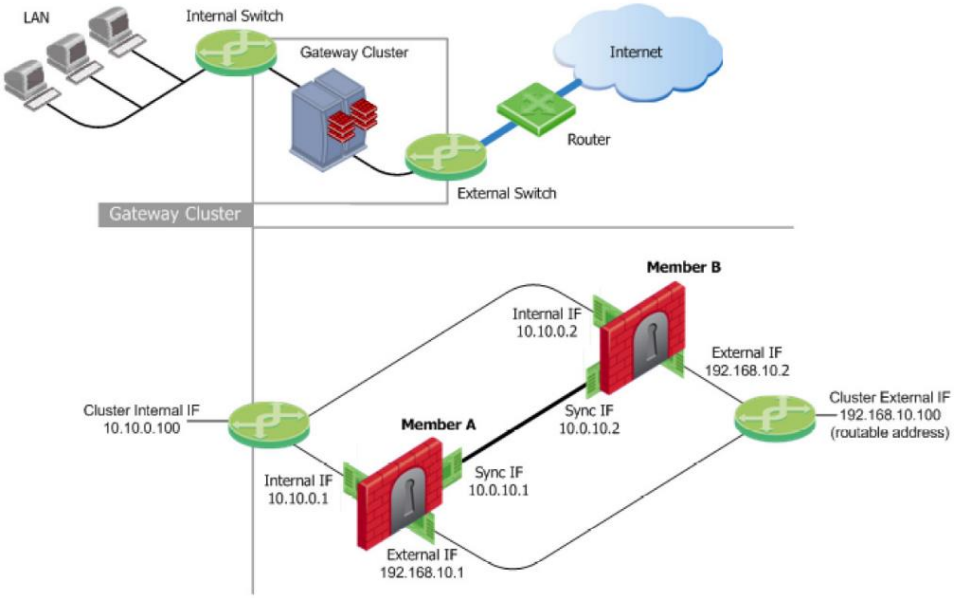
El *Cluster* es un objeto en *SmartConsole*. El tráfico de red puede ser procesado por un miembro del *Cluster* o compartido entre los *Security Gateways* en el *Cluster*. Se pueden configurar hasta ocho miembros en *ClusterXL*.

Cada *Security Gateway/Quantum Spark* del *Cluster* se denomina miembro del *Cluster*. Un miembro del *Cluster* que está procesando el tráfico tiene un estado *Activo*. Uno que no recibe ningún tráfico tiene un estado en *Standby*. El *Cluster Control Protocol* (CCP) conecta y une los miembros del *Cluster* entre sí. Pasa la sincronización y otra información entre los miembros del *Cluster*.

CCP se utiliza específicamente para entornos agrupados para permitir que las puertas de enlace informen sus propios estados y aprendan sobre los estados de otros miembros en el *Cluster*.

El CCP mantiene un *heartbeat* entre los miembros para transmitir que los miembros del *Cluster* están activos y procesan el tráfico de la red. Si después de un tiempo predefinido, no se recibe ningún mensaje de un miembro, se supone que ese miembro está *down* y se produce una *failover* por error. En este punto, otro miembro del *Cluster* asume automáticamente la funcionalidad del miembro que ha fallado.

Nota: El *Cluster Control Protocol* (CCP) es un protocolo patentado de Check Point. Está ubicado entre el *kernel* de Check Point y la interfaz de red.



ClusterXL utiliza direcciones IP y MAC físicas exclusivas para los miembros del *Cluster* y las direcciones IP virtuales para representar el *Cluster* en sí. Las direcciones IP virtuales no pertenecen a una interfaz física en un servidor o dispositivo. Cada miembro tiene tres interfaces: una interfaz externa, una interna y una para sincronización. Las interfaces de los miembros del *Cluster* orientadas en cada dirección se conectan a través de un *switch*, *router*, o *VLAN switch*. Todas las interfaces de miembros del *Cluster* orientadas en la misma dirección deben estar en la misma red.

Nota: no debe haber un *router* entre los miembros del *Cluster*.

El *Security Management Server* se puede ubicar en cualquier lugar y debe ser enrutable a las direcciones de *Cluster* internas o externas.

Todos los componentes del software Check Point deben ser idénticos en todos los miembros del *Cluster*. Esto significa que se habilitan, los mismos *softwares Blades* y *features* en todos los miembros del *Cluster*.

ClusterXL puede instalarse en una configuración en la que los miembros del *Cluster* y el *Security Management Server* estén instalados en diferentes máquinas, o estén instalados en las mismas máquinas.

Si *ClusterXL* está instalado en *Open Servers***,** debe instalarse en una configuración distribuida, en la que los miembros del *Cluster* y *Security Management Server* estén instalados en diferentes máquinas.

ClusterXL se puede desplegar de la siguiente manera:

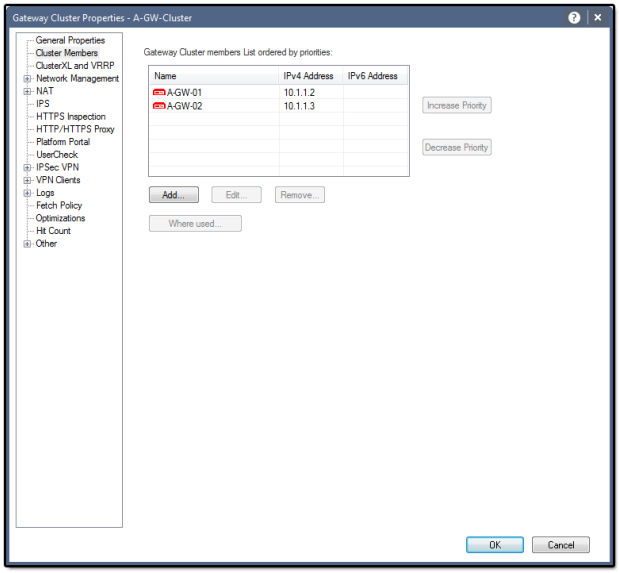
- ***High Availability***: Hay un miembro redundante y solo un miembro está activo a la vez. Conocido como un *Clúster Active / Standby*.
- ***Load Sharing***: Todos los miembros están activos y el tráfico se comparte entre ellos. Conocido como *Cluster Active / Active*.

High Availability proporciona la capacidad de mantener una conexión de red cuando hay un fallo en el *Security Gateway/Quantum Spark* activo o por razones de mantenimiento. Un fallo

ocurre cuando un problema de hardware o software hace que una máquina no pueda filtrar los paquetes. Cuando esto sucede, otro miembro del *Cluster* toma la conexión del miembro activo. En un *Cluster* sincronizado, los miembros en *standby* se actualizan con el estado de las conexiones del miembro del activo.

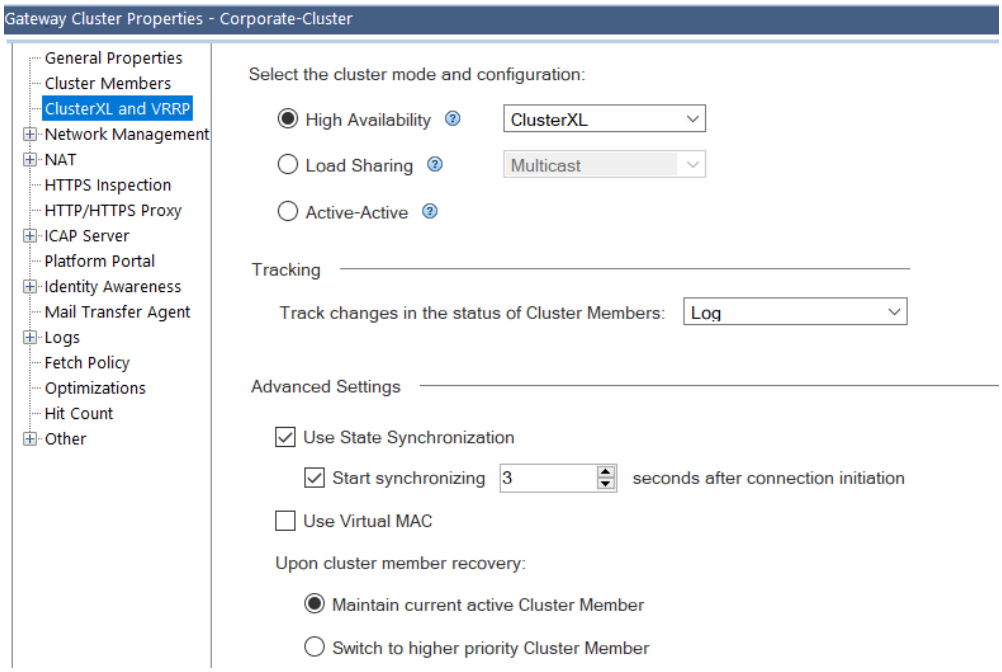
En *SmartConsole*, hay dos pestañas en la ventana "Gateway Cluster Properties" que se utilizan para configurar los ajustes para un *High Availability cluster*: "Cluster Members" y "ClusterXL".

La pestaña "Cluster Members" muestra cada *Security Gateway/Quantum Spark* que es miembro de este *Cluster*. También se usa para configurar la prioridad para cada miembro. Los miembros de *Gateway Cluster* se enumeran en *SmartConsole* por prioridad. El miembro de mayor prioridad es el miembro activo del *Cluster* por defecto. Si este miembro falla, el control pasa al siguiente miembro de mayor prioridad. Si ese miembro del *Cluster* falla, el control pasa al siguiente miembro de mayor prioridad, y así sucesivamente. El miembro en la parte superior de la lista tiene la más alta prioridad. Las clasificaciones de prioridad se pueden modificar en cualquier momento.



En una configuración de Alta disponibilidad, el método de comportamiento debe definirse para cuando se recupera el miembro activo fallido. Las opciones son:

- ***Maintain current active Cluster Member***: se debe seleccionar esta opción si el miembro activo de prioridad más baja debe continuar como el *Security Gateway/Quantum Spark* activo. Esto significa que el miembro que estaba previamente en *standby* antes de *failover* ahora está en modo activo y continuará teniendo el control como miembro activo cuando el miembro activo fallido se recupere. Esta opción se denomina *Active Up* y se recomienda si todos los miembros son igualmente capaces de procesar el tráfico.
- ***Switch to higher priority Cluster Member***: seleccione esta opción si un miembro de mayor prioridad que falló se convierta en el miembro activo del clúster. Esto significa que el Security Gateway/Quantum Spark con la prioridad más alta recuperará el control del miembro de menor prioridad una vez que se recupere. El *Security Gateway/Quantum Spark* de prioridad más baja volverá al modo *standby*. Conocido como *Primary Up*, se recomienda esta opción si un miembro está mejor equipado para manejar conexiones.

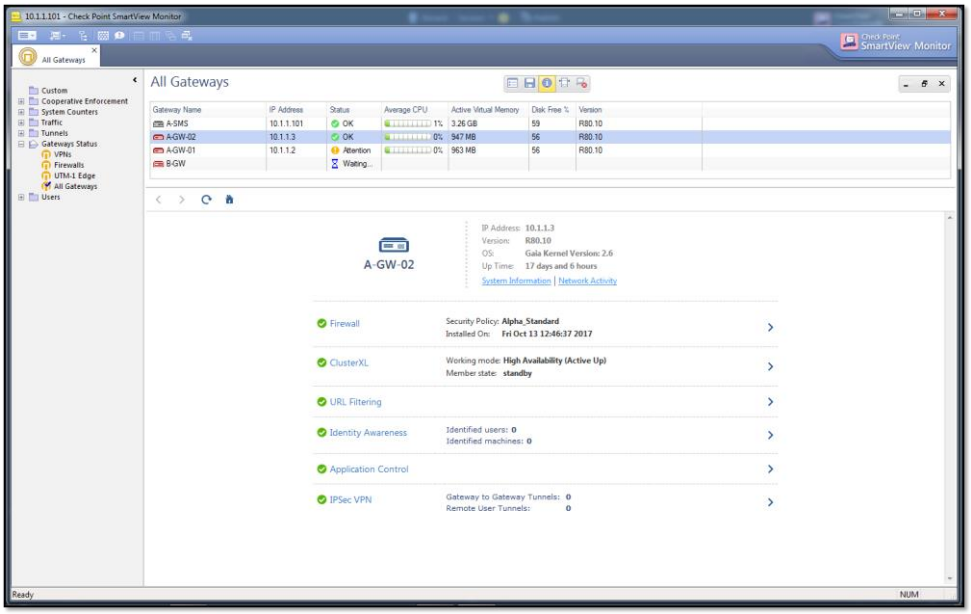


Si hay un problema con un miembro del *Cluster* y ya no puede procesar el tráfico de red, todo el tráfico pasa al siguiente miembro en prioridad. En una implementación de *Active/Standby High Availability*, el estado de las conexiones existentes depende de si el *Cluster* está sincronizado o no.

Se produce un *failover* cuando se produce en el miembro activo:

- Hardware o software falla.
- La política de seguridad no está instalada.
- Mantenimiento planificado.

Puede ser necesario provocar manualmente un *failover*. Use *SmartView Monitor* para detener *ClusterXL* en un *Security Gateway*. En *SmartView Monitor*, con el botón derecho en el *Cluster* y seleccione *Cluster Member* ➔ *Stop Member*.



Por otro lado via CLI, se puede comprobar el estado mediante *cphaprob state*.

```
A-GW-01> cphaprob stat

Cluster Mode:   High Availability (Active Up) with IGMP Membership

Number      Unique Address  Assigned Load   State

1 (local)   192.168.10.2    100%            Active
2           192.168.10.3    0%              Standby

A-GW-01> _
```

Para levantar el miembro del *Cluster*:

```
# clusterXL_admin up
```

Para tirarlo:

```
# clusterXL_admin down
```

7.9 SNMP

SNMP (*Simple Network Management Protocol*) es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. SNMP es un componente de la suite del protocolo de Internet definido por el IETF. Se compone de una capa de aplicación del protocolo, una base de datos de esquema, y un conjunto de objetos de datos.

SNMP en su última versión (SNMPv3) posee cambios significativos con relación a sus predecesores, sobre todo en aspectos de seguridad. Ejemplo de configuración CLI:

```
set snmp agent on
set snmp agent-version any
set snmp community mysnmp read-only
add snmp address <xx.xx.xx.xx>
add snmp traps receiver <yy.yy.yy.yy> community <snmp-community> version v2
add snmp usm user snmp-user security-level authNoPriv auth-pass-phrase-hashed
60a1f34c167b57aff9ac8ee05597
```

```
set snmp usm user snmp-user usm-read-only
set snmp traps trap-user snmp-user
set snmp traps trap authorizationError enable
set snmp traps trap coldStart enable
set snmp traps trap configurationChange enable
set snmp traps trap configurationSave enable
set snmp traps trap fanFailure enable
set snmp traps trap highVoltage enable
set snmp traps trap linkUpLinkDown enable
set snmp traps trap lowDiskSpace enable
set snmp traps trap lowVoltage enable
set snmp traps trap overTemperature enable
set snmp traps trap powerSupplyFailure enable
set snmp traps trap raidVolumeState enable
set snmp traps polling-frequency 5
set snmp traps trap-user snmp-user
set snmp contact "snmp-admin"
set snmp location "Washington Data Center"
```

7.10 BACKUPS

Check Point proporciona varios métodos para realizar copias de seguridad y restaurar el sistema operativo, los parámetros de red y las configuraciones de los dispositivos. Cada método aplica a ciertos parámetros y tiene ventajas y desventajas relativas (tamaño del archivo, velocidad y portabilidad). Para una copia de seguridad completa del sistema se recomienda combinar varios métodos.

7.10.1 SNAPSHOT

Antes de realizar una actualización, puede usar la línea de comando para crear un *snapshot* del sistema operativo o de los paquetes distribuidos. Si falla la operación de actualización o distribución, use la línea de comando para revertir el disco a la imagen guardada. El comando *revert* restaura el sistema desde el archivo de *snapshot* a la misma máquina. La ejecución de la utilidad *snapshot* puede llevar mucho tiempo y puede afectar la producción. Antes de crear un *snapshot*, asegúrese de que haya suficiente espacio libre en la partición de respaldo.

7.10.2 BACKUP (Y SYSTEM RESTORE)

El método de *backup y system restore* se utiliza para restaurar información, que puede restaurarse en una máquina diferente. Funciona de manera muy similar a la utilidad de *snapshot* sin embargo, no afecta la producción. Este método le permite realizar una copia de seguridad de la configuración del sistema operativo Gaia y la configuración de Check Point, así como restaurar una configuración previamente guardada. Un backup puede almacenarse local o remotamente en un servidor SCP.

7.10.3 MIGRATE

El método *migrate*, que también se conoce como método de exportación *upgrade_export/migrate*, realiza una copia de seguridad de todas las configuraciones de Check Point, independientemente del hardware, el sistema operativo o la versión de Check Point. Sin embargo, no incluye información del sistema operativo.

7.10.4 *SAVE CONFIGURATION (AND LOAD CONFIGURATION)*

El método de copia de seguridad *Save Configuration* se utiliza para guardar la configuración de configuración del sistema operativo Gaia, como una secuencia de comandos CLI lista para ejecutar. Le permite revisar su configuración actual y luego restaurar rápidamente la configuración.

El siguiente cuadro proporciona una comparación de los métodos de copia de seguridad.

	Snapshot	System Backup	Migrate	Save Configuration
Does it backup Gaia operating system configuration?	Yes	Yes	No	Yes
Does it backup Products configuration?	Yes	Yes	Yes	No
Does it backup Hotfixes?	Yes	No	No	No
Size of output file on Security Gateway	5 - 100 GB	Depends on configuration	Depends on configuration	Few KB
Size of output file on Security Management Server	5 - 100 GB	5 - 100 GB	Depends on configuration	Few KB
Does it support automatic scheduling?	No	Yes	No	No
Can you restore from different versions?	Yes	No	Upgrade is performed when importing to a newer version	With manual adjustments

Hacer una copia de la configuración del sistema operativo Gaia y la base de datos del Security Management es importante en la administración de una red. Estas copias de seguridad se pueden ejecutar manualmente o se pueden programar.

Todas las copias de seguridad se guardan en un archivo *.tgz* en */var/CPbackup / backups/* en OpenServers */var/log/CPbackup/backups/* en Check Point *appliances*.

También es posible restaurar una copia de seguridad previamente guardada. Las copias de seguridad y las restauraciones pueden realizarse a través de SmartConsole, WebUI o CLI.

7.10.5 BACKUP VIA SMARTCONSOLE

Para realizar un backup en *SmartConsole*, seleccione el *Gateway* desde el que se realizará el backup en la pestaña *Gateways & Servers* y luego seleccione *System Backup* en el menú "Acciones". También es posible realizar un backup de múltiples gateways o servers simplemente seleccionándolos y resaltándolos a todos. Mientras el backup está en progreso, el estado se mostrará en la sesión de tareas en la parte inferior de la GUI. Cuando se completa, pulsar dos veces en la tarea para ver la ruta del archivo y el nombre del archivo de copia de seguridad.

7.10.6 BACKUP VIA WEBUI

Para realizar una copia de seguridad a través de WebUI, expanda “Maintenance” en la vista en árbol, seleccione “System Backup” y “Add Backup”. Seleccionar la ubicación del archivo de copia de seguridad de la lista de tipos de copia de seguridad proporcionada en la ventana “Nueva copia de seguridad”. Para realizar una copia de seguridad a través de WebUI de Quantum Spark, navegue a la pestaña “*Device*”, seleccione “*System*” y “*System Operations*”. Presionar sobre “*Create Backup File*” y una vez generado pulsar sobre “*Download Backup*” para descargarlo.

Antes de restaurar desde una copia de seguridad, la máquina debe configurarse con el nombre de *host* anterior. De lo contrario, se necesita un reinicio doble después de la restauración para activar la máquina.

7.10.7 BACKUP VIA CLI

Se puede acceder al CLI a través de *SmartConsole*. Iniciar sesión en la interfaz de línea de comando para realizar la copia de seguridad.

Use los siguientes comandos para crear y guardar la configuración del sistema:

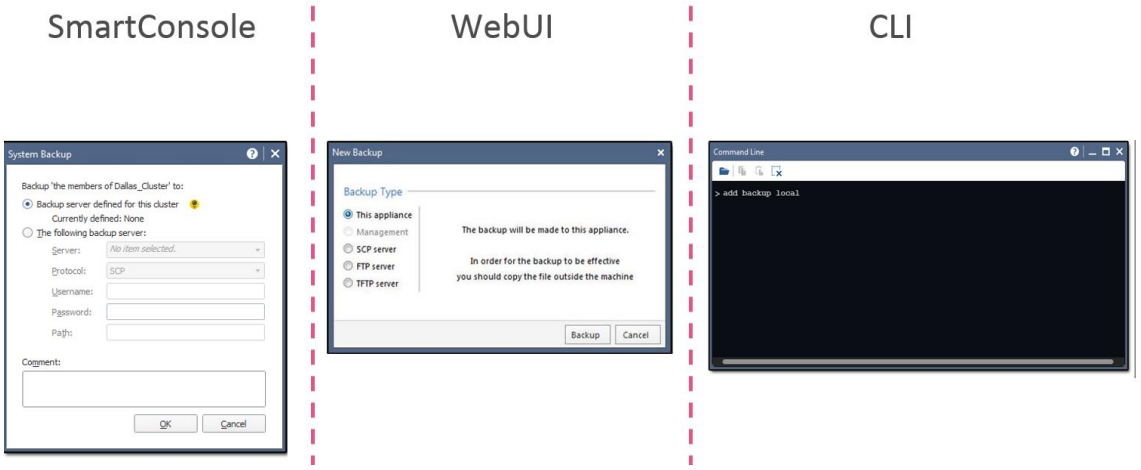
- ***add backup local***: Guarda la copia en /var/CPbackup/backups/
- ***add backup tftp ip <ip>:*** Dirección IP del servidor remoto.
- ***add backup [ftp|scp] ip <ip> username <name> password plain:*** usuario y contraseña del servidor remoto FTP o SCP

Para comprobar mientras se está realizando el backup:

```
show backup status
```

Para ver el estado del backup:

```
show backups
```



7.10.8 AUDITORIA DE CAMBIOS

Cada vez que un administrador inicia sesión en *Security Management Server* a través de *SmartConsole*, comienza una nueva sesión. Durante una sesión, un administrador puede realizar varios cambios en *SmartConsole*, como editar o crear una regla. La regla está bloqueada durante la sesión. Esos cambios se pueden publicar, guardar o descartar. Publicar la sesión actualizará la política. La política debe publicarse antes de poder instalarla. La instalación de la política impulsará los cambios a *Security Gateway*.

Si el administrador publica la sesión, todos los cambios se guardan, se ponen a disposición de otros administradores y se crea una nueva revisión de la base de datos.

Nota: Cualquier cambio realizado por el administrador solo será visible para ese administrador hasta que se publique la sesión.

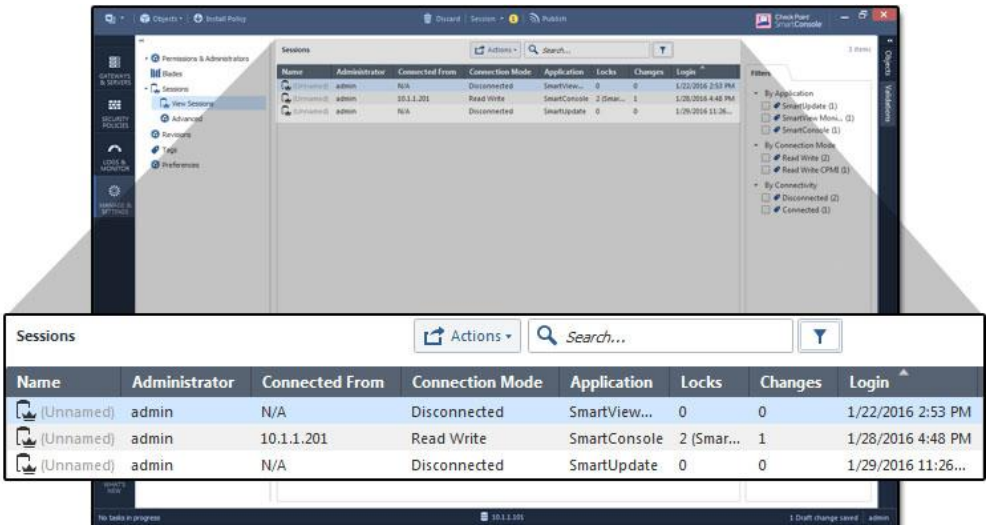
Si el administrador elige descartar la sesión, se pierden todos los cambios. Cuando un administrador intenta cerrar *SmartConsole* sin publicar o descartar cambios, los cambios se guardan como un borrador en el servidor. Se le solicita al administrador las siguientes opciones:

- *Exit*: Lo que permite al administrador acceder a la sesión guardada en el siguiente inicio de sesión.
- *Discard*: Descartar el borrador y salir.
- *Cancel and continue:* Cancelar y seguir con su sesión actual.

Si el administrador guarda la sesión, los cambios hechos en esa sesión están disponibles solo para ese administrador en particular en su siguiente inicio de sesión. Esto presenta un problema si un administrador guarda cambios en objetos o reglas, ya que esos objetos o reglas ahora están bloqueados y otros administradores no pueden editarlos. Un administrador con permiso para administrar otros administradores puede realizar acciones en otras sesiones de administrador, como:

- Publicar y desconectar.
- Descartar y desconectar.
- Desconectar.

Es posible ver una lista de sesiones creadas junto con información detallada sobre cada sesión, como cuántos cambios se realizaron y la cantidad de elementos que están bloqueados. Para navegar a la lista de sesiones, pulse en la pestaña “Administrar” y configuración y luego seleccione “Sesiones” en el árbol de navegación.



7.10.9 ACTUALIZACIONES

Check Point recomienda instalar la versión de software más reciente para mantenerse actualizado con las últimas mejoras funcionales, soluciones de estabilidad, mejoras de seguridad y protecciones contra ataques nuevos y en evolución.

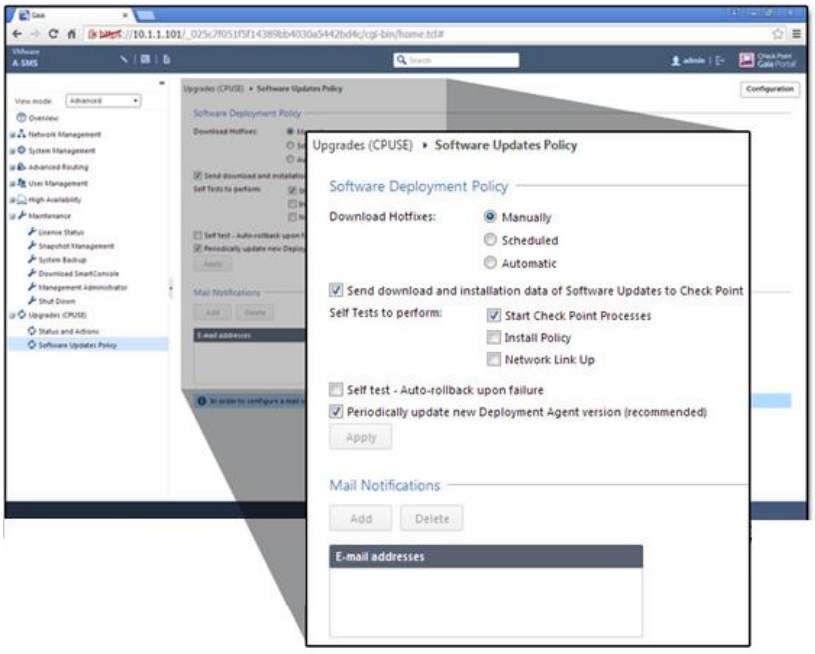
Las actualizaciones proporcionan mejoras adicionales sobre una versión anterior y eliminan las complejidades de volver a crear configuraciones de productos, Políticas de seguridad y objetos. Antes de actualizar los dispositivos o abrir los servidores, verifique la interoperabilidad y la ruta de actualización de su entorno existente y haga uso de las herramientas apropiadas de actualización de Check Point.

Para actualizar de una versión anterior a la R80, se debe realizar una actualización avanzada con el proceso de migración de la base de datos. Las actualizaciones de R80 o superior a R81 se realizan a través del agente de actualización de software, CPUSE.

Nota: IPSO y SecurePlatform no admiten las actualizaciones a R80 y superiores.

Con el motor de servicio de actualización de Check Point (CPUSE), puede actualizar automáticamente los productos de Check Point para el sistema operativo Gaia y el propio sistema operativo Gaia. Las actualizaciones se pueden descargar de forma automática, manual o periódicamente e instalarse manualmente o periódicamente.

Las revisiones se descargan e instalan automáticamente de forma predeterminada, sin embargo, la instalación completa y los paquetes de actualización deben instalarse manualmente.



Para los dispositivos con sistema operativo Gaia Embedded, las actualizaciones se realizan de manera manual a través de la interfaz web. Para ello, navegue a la pestaña "*Device*", seleccione "*System*" y "System Operations". En la sección "*Firmware Upgrade*" es posible actualizar a la última versión pulsando sobre "*Upgrade Now*" o bien proporcionar un fichero de actualización a través de la funcionalidad "*Manual Upgrade*".

7.10.9.1 HERRAMIENTAS DE ACTUALIZACIÓN

Las herramientas de actualización respetan las configuraciones de Check Point, independientemente del hardware, el sistema operativo y la versión de la plataforma de administración de seguridad. Use las herramientas de actualización para hacer una copia de seguridad de las configuraciones de Check Point en las particiones de los dispositivos Check Point y los servidores abiertos. Los requisitos de espacio en disco para las actualizaciones varían según la versión de actualización. Antes de comenzar una actualización, consulte las notas de la versión de la plataforma deseada para verificar los requisitos de espacio para cada partición de disco, como las particiones */var, /log* y */root*.

Hay un paquete diferente de herramientas de actualización para cada plataforma. Descargue la última versión de las herramientas de actualización desde el sitio de soporte de Check Point.

Antes de la actualización, asegúrese de tener un contrato de servicio válido. El paquete de herramientas de actualización consta de varios archivos, incluidos los archivos que figuran en la tabla a continuación.

Descripción del archivo de paquete:

- *migrate.conf*: Mantiene la configuración de la actualización avanzada con la migración de base de datos.
- *migrate*: Ejecuta la actualización avanzada con la migración.
- *pre_upgrade_verifier*: Analiza la compatibilidad de la configuración actualmente instalada con la versión de actualización. Proporciona un informe sobre las acciones a tomar antes y después de la actualización.

- *migrate export*: Realiza copias de seguridad de todas las configuraciones de Check Point, sin información del sistema operativo.
- *migrate import*: Restaura la configuración de la copia de seguridad.

Package File	Description
migrate.conf	Holds configuration settings for Advanced Upgrade with Database Migration.
migrate	Runs Advance Upgrade with migration.
pre_upgrade_verifier	Analyzes compatibility of the currently installed configuration with the upgrade version. It gives a report on the actions to take before and after the upgrade.

7.10.9.2 ACTUALIZACIÓN AVANZADA CON MIGRACIÓN DE BASE DE DATOS

Como en todos los procedimientos de actualización, es una buena práctica actualizar el Servidor de administración de seguridad o el Servidor multidominio antes de actualizar los *Gateways* de seguridad. Para actualizar desde una versión de software anterior, como R77.30, a la plataforma de administración de seguridad R81 de Check Point, use el método "Actualización avanzada con migración de base de datos" para migrar la base de datos e instalar el software. Con este método de actualización, el entorno actual debe cumplir estos requisitos para la migración de la base de datos:

- Espacio de disco disponible de al menos cinco veces el tamaño de la base de datos exportada en la máquina de destino.
- El tamaño de la carpeta */var/log* de la máquina de destino debe ser al menos el 25% del tamaño del directorio */var /log* en la máquina fuente.
- Los servidores de origen y destino deben estar conectados a una red y la interfaz de red conectada debe tener una dirección IP.
- Si los entornos de origen solo usan IPv4 o solo IPv6, el destino debe usar la misma configuración de dirección IP. Por ejemplo, no puede migrar a una configuración de IPv6 si el entorno de origen solo usa IPv4.
- El objetivo debe tener la misma versión o una versión superior y el mismo conjunto de productos instalados.
- El paquete apropiado de herramientas de actualización debe descargarse para cada plataforma fuente.
- Los puertos correctos para *SmartConsole* deben estar abiertos para comunicarse con *Security Management Server*.

7.10.10 LICENCIAMIENTO

Todos los dispositivos y productos de software de Check Point deben contar con la licencia y activación adecuadas antes de su uso.

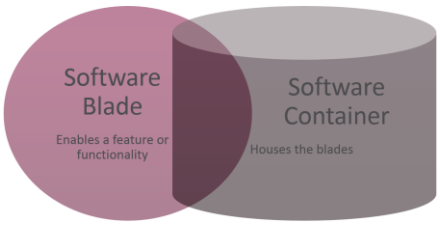
Una licencia contiene las características y la funcionalidad del producto adquirido y especifica sus términos de uso. También contiene otra información, como la cantidad máxima de usuarios, dispositivos y/o direcciones IP asignadas para el producto, así como una *signature key*, *certification key* y datos de contrato de servicio.

Una licencia de software de Check Point consta de dos componentes, el *Software Blade* y el *Software Container*.

Software Blade habilita una característica o funcionalidad específica. Al igual que un servidor físico, el blade de software equivaldría a un servidor *blade* físico. Cada *blade* debe estar conectado a un contenedor de software.

Software Container alberga los *blades*. Permite la funcionalidad del servidor y define su propósito como el de un servidor de administración o G*ateway*. Hay tres tipos de contenedores de software: *Security Management, Security Gateway*, y *Endpoint Security*. Los *blades* del *Security Management* y *Security Gateway/Quantum Spark* se deben conectar a un contenedor de software para obtener una licencia. Los módulos de software de *Endpoint Security* se licencian independientemente del *Endpoint Security Container*.

Todas los *blades* como parte de una solución específica se conectan automáticamente a al menos un contenedor. No es posible separar *blades* en paquetes. Cuando un *blade* de software se compra por separado de un paquete, se lo conoce como *blade* "a la carta". Por ejemplo, si desea agregar la función de *SmartProvisioning* a su solución de gestión de seguridad existente, debería comprar una *SmartProvisioning Blade* a la carta.



Security Management y *Security Gateway/Quantum Spark software blade licenses* son perpetuas, lo que significa que no tienen fecha de caducidad. Los *blades* de software de *Security Gateway/Quantum Spark* tienen licencia por *Gateway*, mientras que los *blades* de software de *Security Management* requieren una licencia de *blade* de administración por contenedor de administración, independientemente del tamaño del contenedor.

Los *blades* de servicio, como IPS, *URL Filtering*, y *Application Control* se consideran *blades* de suscripción. Las licencias para *blades* de suscripción pueden caducar. La licencia incluye tanto la suscripción de software como el Contrato de Servicios de Soporte asociado. Estos *blades* se licencian y renuevan durante un período de tiempo específico, que suele ser de 1, 2 o 3 años.

Los *blades* de software de *Endpoint* están disponibles como *blades* perpetuos y de suscripción, sin embargo, el contenedor siempre es perpetuo. *Endpoint* es único ya que requiere un contenedor de administración y un contenedor de punto final. Todos los productos de *Endpoint* se licencian independientemente de *Endpoint Security Container* y las licencias se instalan en el servidor de administración de *Endpoint*.

Nota: Para *Endpoint*, el blade de acceso remoto está instalado en el Servidor de administración de seguridad de red en lugar del Servidor de administración de endpoint.

Las licencias adicionales incluyen licencias *Plug-and-Play* (de prueba) y licencias de evaluación. Una licencia *Plug and Play* brinda una licencia temporal por 15 días de funcionalidad completa

ilimitada para el usuario después de comprar e instalar su dispositivo. Estas licencias le permiten activar su licencia permanente en un momento posterior.

Las licencias de evaluación se generan con el fin de evaluar productos antes de comprar. Estas licencias proporcionan funcionalidad completa ilimitada para el usuario durante 30 días. Cuando caducan los 30 días, la funcionalidad del software está deshabilitada.

Las Licencias Check Point se presentan en dos formas: Central y Local.

La **Licencia Central** es el método de licencia preferido y recomendado. Esta licencia relaciona la licencia del paquete con la dirección IP del *Security Management Server* y no tiene dependencia de la IP del *Gateway*. Esto significa que solo hay una dirección IP para todas las licencias y la licencia sigue siendo válida incluso si se cambia la dirección IP del *Gateway*. La licencia se puede tomar fácilmente desde un *Gateway* y entregársela a otro. No es necesario crear e instalar una nueva licencia.

Una **Licencia Local** está vinculada a la dirección IP de un *Security Gateway/Quantum Spark* específico. Esta licencia no se puede transferir a aun nuevo *Gateway* con una dirección IP diferente. Una licencia local solo se puede usar con un *Security Gateway/Quantum Spark* o un *Security Management* con la misma dirección.

Las licencias centrales requieren que un administrador designe un *Gateway* para el archivo adjunto, mientras que las licencias locales se conectan automáticamente a sus *Gateways*.

7.10.10.1 ACTIVACIÓN DE LICENCIAS

Una vez que los *blades* necesarios están conectados, ya sea por Check Point o por el administrador de cuentas de la organización, la licencia del servidor de administración está lista para activarse. Check Point ofrece dos métodos para activar una licencia: activación online y activación offline.

La **activación online** está disponible para los dispositivos fabricados por Check Point. Usando el Asistente de configuración de por primera vez de Gaia, el dispositivo se conecta al Centro de usuario de Check Point y descarga todas las licencias y contratos necesarios. No se requieren más pasos para licenciar el dispositivo. El Centro de usuario es un portal de administración de inicio de sesión único que brinda soporte técnico, otros recursos y herramientas para administrar cuentas y productos de Check Point. La activación en línea no se puede usar para *open servers* y dispositivos que no sean de Check Point, como dispositivos de la serie IP o soluciones de dispositivos integrados de IBM.

Aunque es opcional, el dispositivo debe estar configurado para tener conectividad a Internet durante la finalización del asistente de configuración para poder conectarse al Centro de usuario. Si el dispositivo no tiene acceso directo a Internet, la configuración del proxy se puede configurar en la página de Información del dispositivo en el asistente de configuración.

La **activacion offline** está disponible para todas las instalaciones de Check Point. Un *Account Administrator* o *Licenser* generará un archivo de licencia a través del Centro de usuarios de Check Point y luego aplicará la licencia a través de *SmartUpdate*, una aplicación dentro de SmartConsole.

Las licencias para los productos de hardware de Check Point son válidas solo como parte de la vida del producto designado originalmente. Los dispositivos incorporados de Gaia adquiridos con una solución empaquetada incluirán las licencias de software especificadas y el contenedor de software asociado. Ambas opciones de activación en línea y fuera de línea están disponibles para los dispositivos Check Point integrados en Gaia.

El licenciamiento automático permite tener todas las licencias activadas automáticamente. Esta opción solo se puede aplicar a dispositivos Check Point. Para usar esta característica, el servidor de administración debe poder conectarse a Internet. La función de licencia automática realiza las siguientes operaciones:

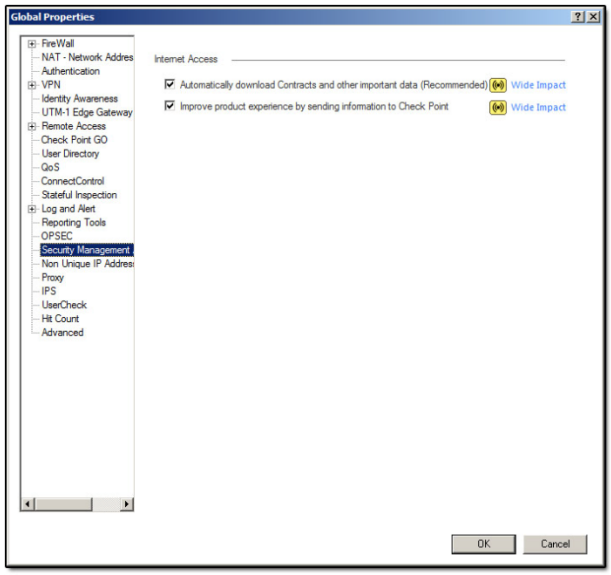
- Verificaciones periódicas de las licencias.
- Activa nuevas licencias agregadas al Depósito de Licencias y Contratos.
- Agrega automáticamente nuevos *blades* a *SmartConsole*.

Para activar la función de Licencia automática:

1. Iniciar SmartConsole.

2. Desde el menú “Iniciar”, seleccione “Global Properties” y posteriormente “Security Management Access”.

3. Pulsar en el *checkbox* de “Automatically download Contracts and other important data”.



Después de generar una licencia, debe estar instalada en el *Gateway* y registrada con el *Security Management Server*. Las licencias de Check Point se pueden instalar a través de *SmartUpdate*.

Para instalar una licencia, primero debe agregarla al "Repositorio de Licencia y Contrato". Para agregar una licencia:

- Iniciar SmartUpdate.
- Elegir la pestaña "Licenses & Contracts"
- Desde el menú de inicio, elegir Licenses & Contracts ➔ Add License.
- Se recomienda instalar licencias a través de SmartUpdate; sin embargo, también es posible instalar una licencia a través de la CLI. Use el siguiente comando para verificar que la licencia esté instalada: cplic print

Hay tres formas de agregar una licencia al Depósito de licencia y contrato: desde el Centro de usuario, desde un archivo o manualmente.

Añadir Licencia desde el *User Center:*

- Pulsar en "Add Licenses" desde el icono "User Center", o desde el "Menu", elegir *Licenses & Contracts -> Add License* ➔ *From User Center.*
- La ventana del navegador abrirá la página de inicio de sesión de "Check Point User Center / PartnerMap".
- Iniciar sesión con sus credenciales para descargar el archivo de licencia del *User Center*.
- Después de descargar el archivo, regrese a *SmartUpdate* para agregar la licencia a "License & Contract Repository" usando "From File" o "Manually method".

Añadir Licencias desde Archivo:

- Pulsar en "Import Licenses" desde el icono de "Archivo", o desde el "Menú", elegir *Licenses & Contracts* ➔ *Add License* ➔ *From File*.
- Navegar hasta la localización del archivo de licencia y seleccionar "Abrir".

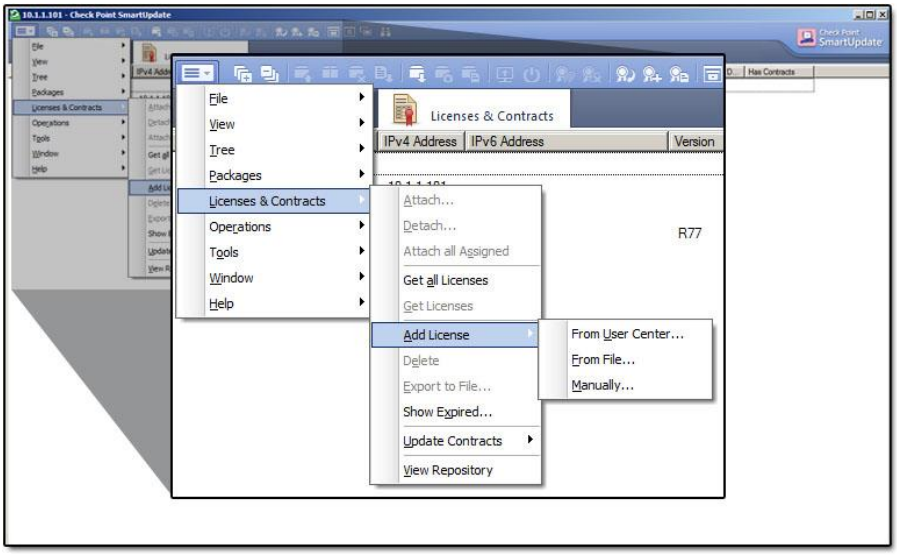
- Las licencias Locales serán automáticamente añadidas al *Security Gateway*. Las licencias Centrales se almacenan en el repositorio *License & Contract Repository*.
- Las licencias locales se adjuntarán automáticamente a *Security Gateway*. Las licencias centrales se colocarán en el repositorio de licencias y contratos.

Nota: Las opciones del nombre del archivo de licencia pueden variar ligeramente entre versiones.

Añadir Licencia Manualmente:

Al generar una licencia, se enviará al administrador de la cuenta un correo electrónico que contiene el archivo de licencia y las instrucciones de instalación manual para agregar la licencia al depósito de licencias y contratos. Para agregar una licencia de forma manual:

- Copie la cadena de licencia de su correo electrónico al portapapeles. La cadena comenzará con *cplic put* y finalizará con la última SKU/característica. Por ejemplo: *cplic put 1.1.1.1 10march2018 dw59Ufa2z-eLLQ9NBgP-uyHzvQWKr-HeSo4zLQx CPSG-C-2-U CPSB-FW*.
- Seleccionar la pestaña *License&Contracts* en *SmartUpdate*.
- Pulsar en el icono "Agregar" licencia manualmente, o desde el Menú de inicio, elegir *Licenses & Contracts* ➔ *Add License* ➔ *Manually*. Aparecerá la ventana "Add License".
- Puede asignar un nombre a la licencia, si lo desea. Si deja el campo Nombre vacío, a la licencia se le asigna un nombre en el formato *SKU @ fecha*.
- Puede escribir los detalles de la licencia o pulsar "Pegar Licencia" en cuyo caso los campos se completarán con los detalles de la licencia.
- Pulsar en "Calculate" y asegúrese de que los resultados coincidan con el código de validación recibido del Centro de usuario. El código de validación se usa para confirmar la licencia.
- Pulsar en "Aceptar" para completar la operación.

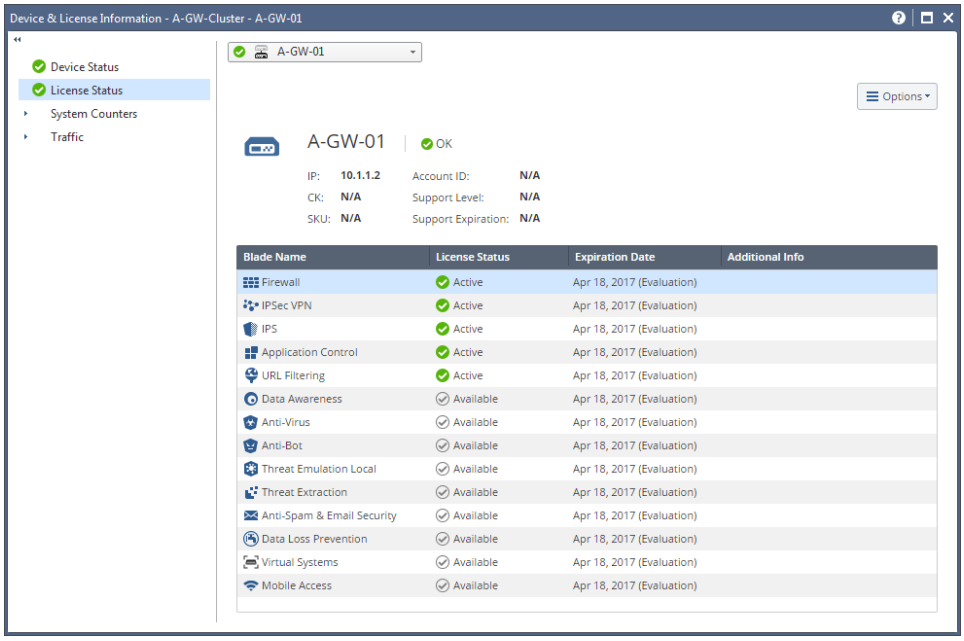


SmartConsole le permite hacer referencia rápidamente al estado de la licencia para cada *blade* por *Gateway*. La vista "Estado de licencia" proporciona información sobre cada blade y resume

qué productos o servicios están activos y/o disponibles para el Gateway. Para ver el estado de la licencia:

- En *SmartConsole*, pulse en el objeto que desea ver.
- Desde la pestaña "*Summary*", pulse en "*Device & License Information*".
- Aparecerá la ventana de "*Device & License Information*". Pulsar en la opción "License Status" ubicada en el panel de la izquierda.

También puede guardar la información de estado como un informe PDF o exportar la información a un archivo.

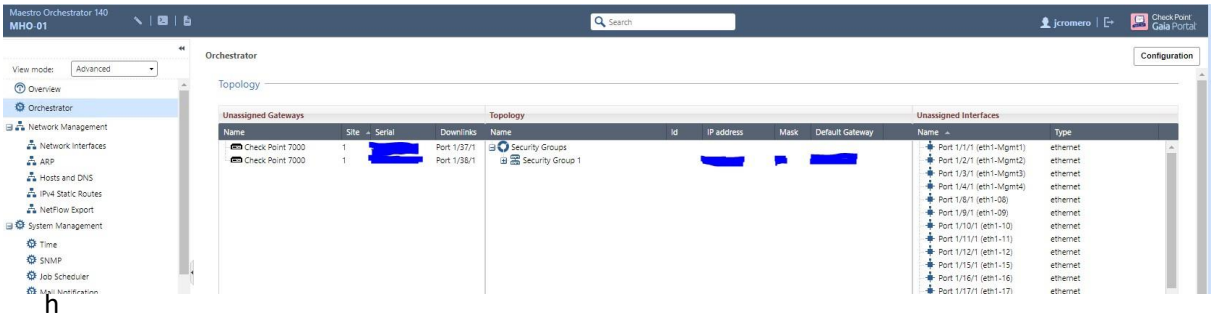


8. CONFIGURACIÓN DE EQUIPO MAESTRO

8.1 CONFIGURACIÓN DEL SECURITY GROUP

La configuración del Security Group se puede realizar vía WebUI o vía Clish en los orquestadores. El nombre de las interfaces del orquestador depende del member ID que tenga dicho orquestador, por lo que el member_id 1 tendrá interfaces Port 1/X/Y (eth1-X) y el member_id 2 tendrá interfaces Port 2/X/Y (eth2-X). Para ello, se seguirán los siguientes pasos:

1. Abrir *https://<ip_mgt_mho1>*
2. Ir al menú "*Orchestrator*" y se accede a una pantalla como la siguiente:

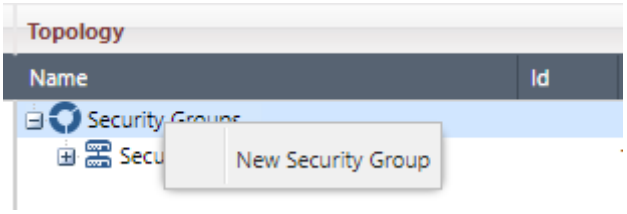


h

En dicha pantalla aparecen tres columnas:

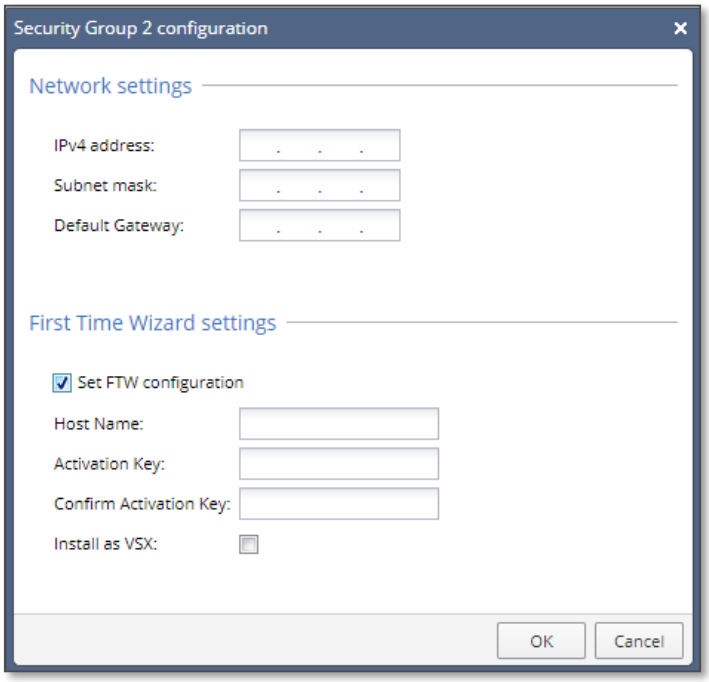
- *Unassigned Gateways:* appliances descubiertos por LLDP y que están sin asignar a ningún SG.
- *Topology*: Security Groups existentes.
- *Unassigned Interfaces*: Interfaces de uplink y gestión de SG que están disponibles para utilizar. Comentar que los interfaces de Downlink no figuran y son visibles pasando el ratón por encima de los appliances (es información que se obtiene mediante LLDP).

3. Botón derecho en *Security Groups* y seleccionamos "*New Security Group*"



4. Se cumplimenta la información solicitada:
   - *Network settings*: será la dirección IP de gestión del SG.

- *FTW*: activar el FTW y añadir la información sobre Host Name, SIC y si es VSX o normal appliance.



5. Seleccionar los appliances que formarán parte del *Security Group* y arrastrarlos desde la columna "*Unassigned Gateways*".
6. Seleccionar las interfaces que formarán parte del *Security Group* y arrastrarlas desde la columna "*Unassigned Interfaces*"
    a. Interfaz de Gestión del SG (por ejemplo, Eth1-Mgmt1).
    b. Interfaces de Uplink.
7. Presionar "*Apply*". En este punto los appliances se reiniciarán para levantar el *Security Group* con la configuración facilitada. Una vez hayan levantado, el *Security Group* debería estar accesible desde la IP de gestión del SG por https y ssh.
8. Una vez creado el *Security Group* (6 minutos aproximadamente), se puede acceder por ssh, https o moviéndose desde el orquestador con el comando "m". Desde el modo expert del MHO:

    [Expert@<hostname MHO>:0]# m <id SG> <appliance_id> (por ejemplo, m 1 1)

9. Comprobar que el SG se ha creado correctamente:

```
hostname MHO> show maestro security-group
id <sg_id> hostname MHO> expert
```

8.2 CONFIGURACIÓN DE GAIA DEL SECURITY GROUP

La configuración necesaria a nivel sistema operativo Gaia del Security Group sigue el mismo procedimiento que se realiza con cualquier gateway de Check Point y mismo sistema operativo.

En este apartado se configurarán aspectos como, por ejemplo:

- Interfaces (físicas, lógicas, bondings,…) y su direccionamiento IP, ARP, DNS.
- Routing estático y dinámico.
- NTP, SNMP, DHCP, Syslog.
- Usuarios locales

Una vez se haya realizado esta configuración, el security Group ya estaría listo para ser integrado con el entorno de gestión.

8.3 CONFIGURACIÓN DESDE EL ENTORNO DE GESTIÓN

La configuración necesaria en el entorno de gestión para dar de alta el Security Group sigue el mismo procedimiento que se realiza con cualquier gateway de Check Point (nuevo Gateway, establecimiento del SIC, revisión de la topología, configuración de políticas, activación de blades, etc.). La dirección IP a utilizar en el objeto será la dirección IP de gestión del Security Group.

Una vez se haya terminado el alta del Security Group en el entorno de gestión y se haya realizado la instalación de políticas, podremos comprobar como todos los appliances del Security Group están Activos.

9. PLANO DE CONTROL DE ACCESO

En este apartado se tratarán las funcionalidades existentes en el plano de control de acceso. Entre ellas, funcionalidades de control del uso de aplicaciones, la perdida de datos sensibles, la identificación de direcciones IP con usuarios y máquinas, etc.

9.1 IDENTIFICACIÓN DE USUARIOS: IDENTITY AWARENESS

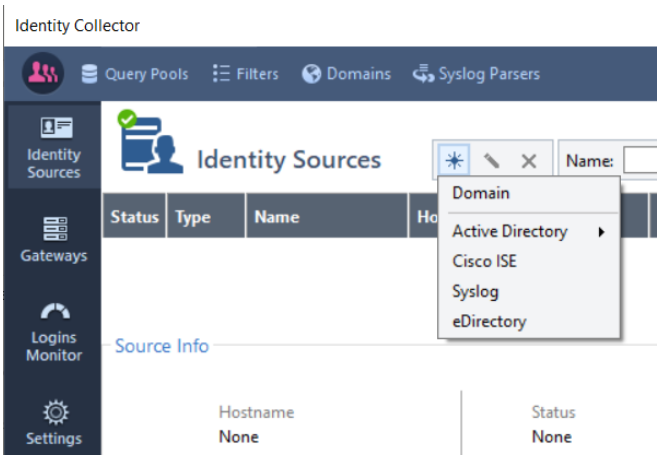
Existen varios métodos para obtener la identidad del usuario, incluyendo: *clientless*, *captive portal* o *identity agent*, *ADQuery Agent* , *IF-MAP* o *API REST*.

- *Clientless*: se basa en la integración con el Directorio Activo, es transparente para el usuario. Existen dos variantes: en la primera el propio *Security Gateway/Quantum Spark* se conecta al Directorio Activo y establece las relaciones usuario/máquina/IP que podrá compartirlas con otros dispositivos Check Point en la red; en la segunda se dedica una máquina Windows del dominio a extraer esa información y compartirla con el cortafuegos, esta opción es la recomendada con más de 5000 usuarios o 50 servidores de directorio.

- *Captive portal:* se usa para adquirir la identidad de usuarios desconocidos, que no forman parte del dominio. El usuario se identifica a través de un portal web antes de poder acceder a los recursos, que se le asignan a través de perfiles de usuario.

- *Identity agent*: es un agente dedicado instalado en los ordenadores de los usuarios para adquirir e informar de la identidad al *Security Gateway*. *Identity Agent* proporciona autenticación transparente usando el *Single Sign-On* de Kerberos cuando los usuarios entran en el dominio; así como seguridad adicional, gracias a la tecnología *packet tagging* que permite marcar los paquetes para protegerlos contra ataques de IP *Spoofing*.

- *Radius accounting:* mediante el análisis de los *logs* del Radius, obtiene la información de identidad de las peticiones del cliente Radius. *Identity Awareness* utiliza esta información para obtener la información de usuario y grupo del servidor LDAP.
- IF.MAP: Check Point proporciona la posibilidad de integración con repositorios IF-MAP, pudiendo utilizar el servidor IF-MAP como elemento de transferencia de identidades de elementos que actualmente no presentan una integración completa con Check Point.
- *ADQuery Agent*: se trata de un agente pensado para entornos complejos y con un número muy alto de identidades. El objetivo es eliminar la necesidad de hacer uso de los recursos del *Gateway* para captar las entidades, y de esta forma reducir el impacto de performance en el propio *Gateway*. Dicho agente no hace uso de WMI, sino que utiliza una Windows API, minimizando el impacto en performance sobre el AD y evitando la necesidad de hacer uso de un usuario administrador del dominio. Dicho agente se puede instalar sobre el propio controlador de dominio o sobre cualquier equipo Windows de la red.
- API REST: en este caso, se proporciona una forma sencilla de dar de alta o baja asociaciones usuario/máquina/IP de manera automatizada para integrar esta gestión de usuarios con otras aplicaciones o directorios propietarios.
- *Identity Collector*: la forma recomendada cuando sea posible. Se trata de un agente basado en Windows que se encarga de recolectar información acerca de identidades y sus direcciones IP asociadas, enviándolas a los *Security Gateways* de Check Point para la aplicación de las reglas de seguridad basadas en identidades. Identity Collector soporta diferentes fuentes de identidades como:
    - Controladores de Directorio Activo.
    - *Cisco ISE (Identity Services Engine) Servers*
    - Mensajes de *Syslog*
    - *NetIQ eDirectory*

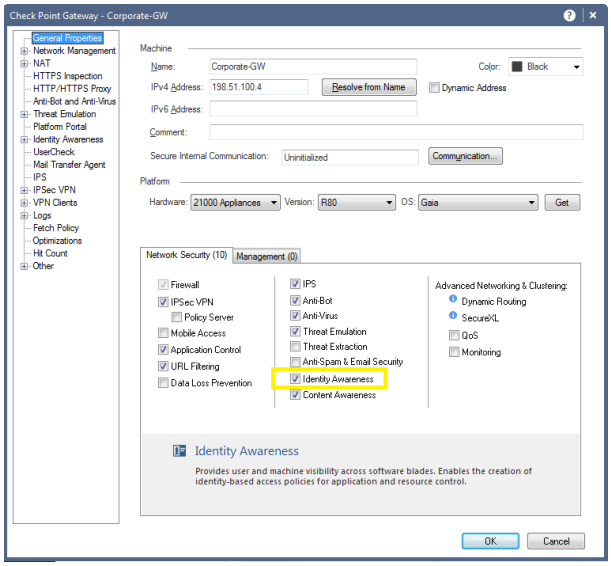


La información acerca de la identidad de usuarios y máquinas puede ser compartida de forma sencilla, según se necesite en un *Gateway* o a través de toda la red. Los beneficios de compartir dicha información incluyen:

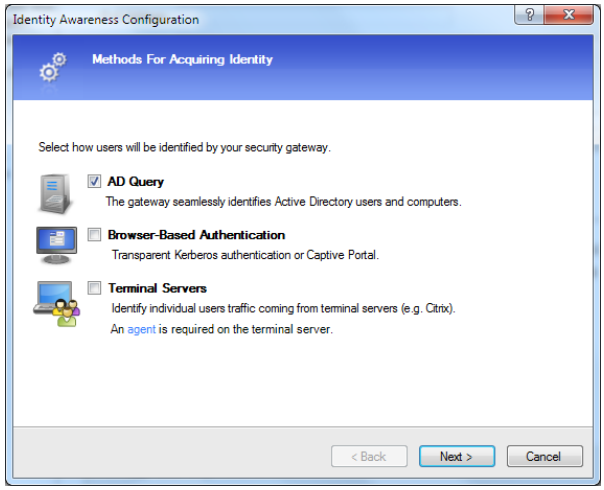
- Autenticación única de usuario: la identidad del usuario es compartida entre todos los *Gateways*, permitiendo a los usuarios acceder los recursos que tienen asignados desde cualquier lugar de la red.
- Previene la saturación de la red al evitar búsquedas repetidas en el Directorio Activo.
- Simplifica la implementación de los servidores *Active Directory* y su sincronización.

Para configurar Identity Awareness:

1.- Primero se debe habilitar el *software blade* de "Application Control" en el *Security Gateway/Quantum Spark* correspondiente:



2.- Seguir el *wizard* Inicial:



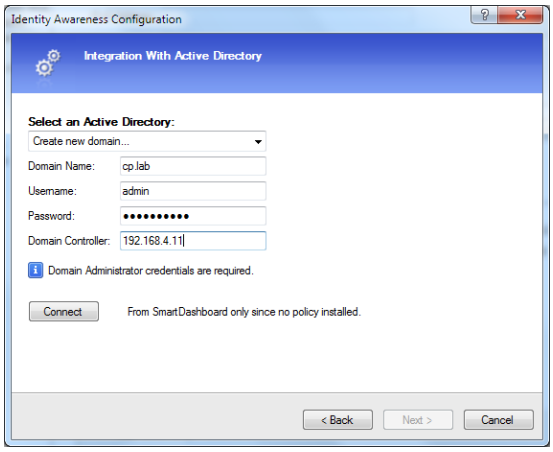
3.- Se puede seleccionar distintos métodos de adquisición de identidades:

- AD Query: A través del Active Directory.
- Browser-Based Authentication: A través de portal cautivo o ticket Kerberos.

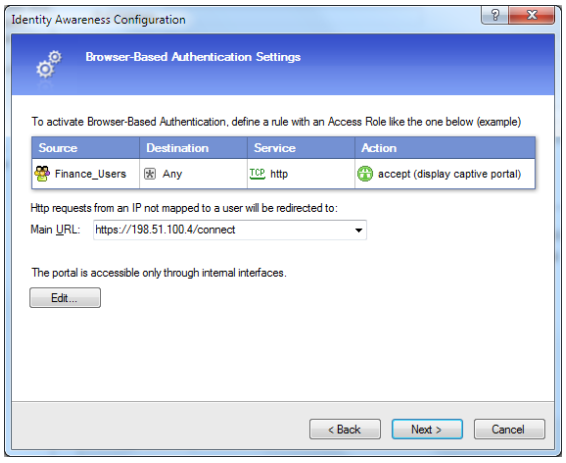
- Terminal Server: Identificando el tráfico de usuarios a través de Terminal Server como por ejemplo Citrix. Es necesario un agente en el Terminal Server.

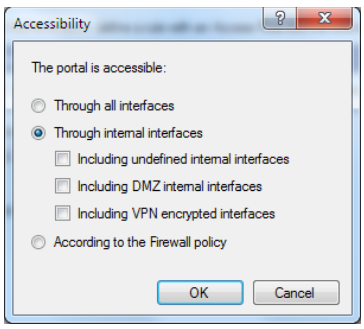
4.- Configurar la integración con el *Active Directory*, utilizando los parámetros:

- Nombre de Dominio.
- Usuario de administración del *Active Directory*.
- *Password*.
- IP del *Domain Controller*.



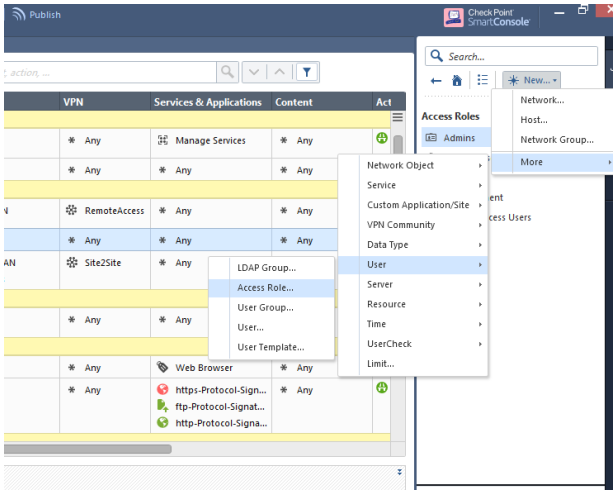
5.- Configuración del portal cautivo, URL a la que se redirigirá e interfaces desde las que se mostrará el portal cautivo (interfaz externa del *Gateway* por defecto).





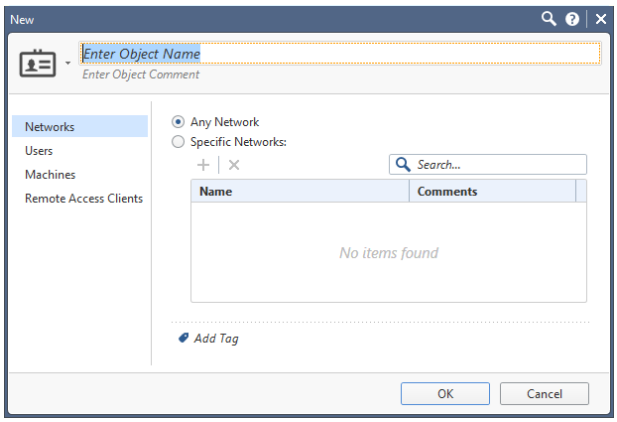
6.- Pulsar en "*Next*" y el *blade* de *Identity Awareness* quedará activado.

Para poder utilizar la identificación de usuarios en las Políticas de seguridad hay que crear un *Access Role*: *New* ➔ *User* ➔ *Access Role*.

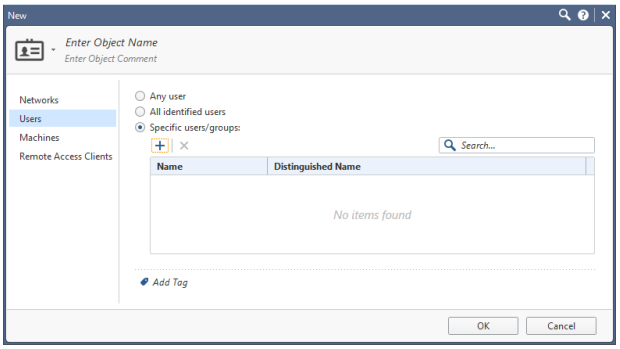


Al crear un nuevo *Access Role* se deben establecer los siguientes parámetros:

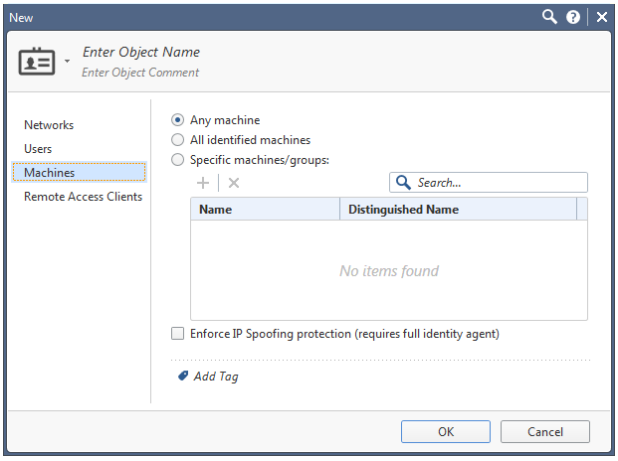
- Nombre del *Access Role*.
- Redes a las que pertenecerá dicho *Access Role*



Usuarios que pertenecerán a dicho *Access Role:*

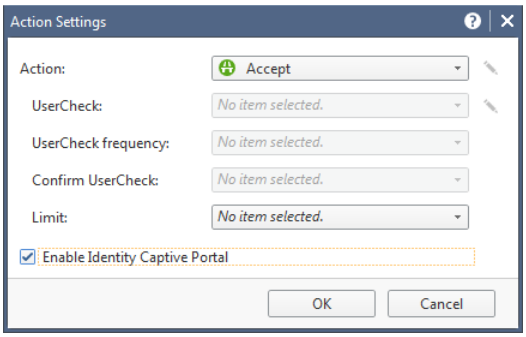


Se puede restringir el acceso no sólo por usuario sino desde qué máquina esté conectado dicho usuario.



Una vez creado el *Access Role* puede ser utilizado tanto en el origen como en el destino de las reglas de seguridad.

Para configurar que se lance el portal cautivo en una determinada regla de seguridad es necesario irse a la columna de “Action”, pulsar “More” y habilitar “Enable Identity Captive Portal”.



9.2 VPN

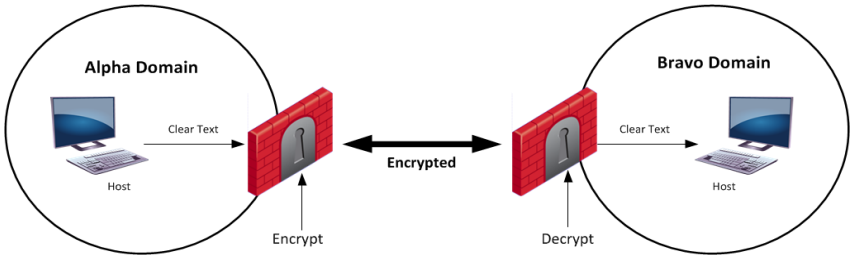
Los túneles VPN se utilizan para proporcionar privacidad y seguridad cifrando conexiones y datos.

Un ejemplo de uso puede ser los usuarios de una organización que requieren descargar archivos y consultar el correo electrónico cuando están fuera de la oficina.

La solución Check Point VPN garantiza la autenticidad mediante el uso de métodos de autenticación estándar para transferir información y datos. Proporciona privacidad, cifrando todos los datos enviados a través de la red. También tiene integridad con el uso de protocolos estándar de la industria que aseguran que los datos estén seguros y protegidos.

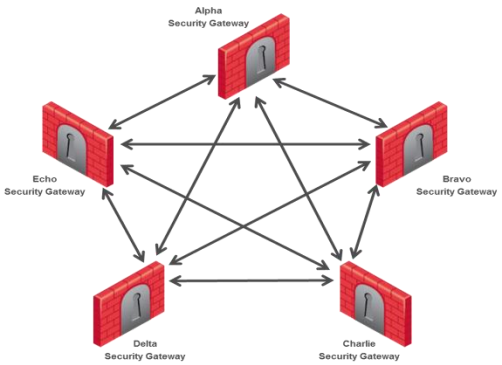
Los siguientes componentes se usan para construir una VPN:

- Dominio VPN: Incluye las computadoras y redes que se definen como los recursos internos conectados al túnel VPN.
- Gateway VPN: Encripta y protege los recursos en el dominio VPN. Un *Security Gateway/Quantum Spark* con el *blade* de software VPN habilitado también se denomina *Gateway VPN*. En las implementaciones de VPN "site-to-site", todas las pasarelas de seguridad son puertas de enlace VPN.
- Comunidad VPN: Incluye dominios VPN que comparten de forma segura los recursos de la red. Los tipos de comunidades de VPN incluyen *Star*, *Meshed* y Acceso Remoto.
- Entidades de confianza de VPN: Incluye certificados y *shared secrets*. El ICA de Check Point se puede usar para proporcionar certificados para *Gateways* de seguridad internos y clientes de acceso remoto.
- Herramientas de administración de VPN: Incluye *Security Management Server* y *SmartConsole*, que permiten a las organizaciones definir e implementar fácilmente túneles VPN de sitio a sitio y acceso remoto.

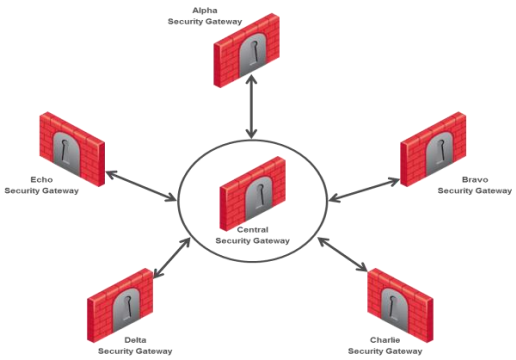


Hay tres tipos de comunidades de VPN: Malla, Estrella y Combinación de ambas.

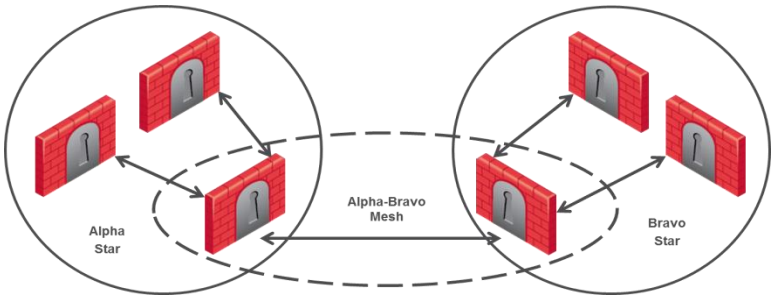
- Comunidad VPN mallada: consiste en *VPN Gateways* que crean túneles VPN con todos los otros *VPN Gateways* de la comunidad. A menudo se utiliza para una intranet corporativa, a la que solo pertenecen las oficinas corporativas.



- Comunidad VPN en estrella: Consta de uno o más VPN Gateways centrales y satelitales. En este tipo de comunidad, un satélite puede crear un túnel VPN solo con otros dominios VPN donde el VPN Gateway se define como central. Un VPN Gateway satelital no puede crear un túnel VPN con otro VPN Gateway que también se define como satelital.



- Combinación de Comunidades VPN: Hay escenarios de implementación de VPN más complejos. Por ejemplo, una comunidad de VPN combinada utilizando dos comunidades de VPN estrella y una comunidad VPN mallada.



Al crear una comunidad VPN, además de configurar en los cortafuegos de origen y destino para usar los túneles VPN, aún es necesario configurar las reglas en la política de control de acceso para permitir las conexiones entre los *VPN gateways*.

9.2.1 IPSEC VPN

Check Point utiliza el conjunto de protocolos IPSec para gestionar túneles de comunicación cifrados. Un componente clave de IPSec es IKE. IKE es un protocolo estándar que crea los túneles VPN y administra las claves utilizadas para cifrar y descifrar datos e información.

IPSec utiliza *Authentication Header* (AH), *Encapsulating Security Payloads* (ESP) y *Security Associations* (SA) para autenticar y encriptar paquetes IP para comunicaciones VPN. El protocolo AH autentica el encabezado IP y los datagramas, proporcionando integridad sin conexión y garantizando que el encabezado y la carga útil no se hayan modificado desde la transmisión. ESP opera directamente sobre IP y proporciona autenticidad de origen, integridad y protección confidencial de los paquetes. SA proporciona el conjunto de algoritmos y datos que establece los parámetros para usar AH y ESP. Con las SA, los administradores de seguridad

pueden administrar exactamente qué recursos se pueden comunicar de forma segura según la Política de seguridad.

El protocolo IKE se usa para configurar una SA en el conjunto de protocolos IPSec. La configuración requiere que los paquetes IPSec primero se autentiquen y establezcan claves compartidas IKE. Para ofrecer una sesión de comunicación segura y garantizar la autenticación y la confidencialidad, IKE lleva a cabo un proceso de negociación en dos fases utilizando algoritmos de autenticación y cifrado acordados entre las dos computadoras.

- **Fase 1 (*Main Mode*):** Protege la identidad de los dos *peers*. Negocia el algoritmo de cifrado, el algoritmo *hash*, el método de autenticación y el grupo *Diffie-Hellman* (DH). Durante esta fase, los pares IPSec se autentican y establecen un canal seguro para la comunicación. El siguiente proceso ocurre:
  1. Se negocian todos los métodos de autenticación, los algoritmos de cifrado y los grupos *Diffie-Hellman*.
  2. Cada puerta de enlace genera una clave privada DH y las claves públicas y calcula las claves compartidas.
  3. Se realiza la autenticación de los extremos y se establece un túnel seguro para negociar los parámetros IKE fase 2.
- **Fase 2 (*Quick Mode*):** Las SA se negocian, se determina la clave compartida y se produce un DH adicional. Una vez que las dos computadoras llegan a un acuerdo, se establecen dos SA, una para la comunicación saliente y la otra para la comunicación entrante. El siguiente proceso ocurre:
  1. Se intercambia más claves y se acuerdan los parámetros de encriptación y autenticación IPSec.
  2. La clave DH se combina con el resto de claves para producir la clave IPSec simétrica.
  3. Se generan las claves IPSec.

9.2.2 VPN SITE-TO-SITE

Maneja la comunicación segura entre las oficinas que están conectadas por Internet. A través de un túnel VPN encriptado. Dos *Gateways* VPN negocian un enlace y crean un túnel VPN. Cada túnel puede contener más de una conexión VPN. Además, una pasarela VPN puede mantener más de un túnel VPN al mismo tiempo. Los terminales de túneles en ambas extremos realizan la negociación IKE y crean un túnel VPN. Utilizan el protocolo IPSec para cifrar y descifrar el mensaje.

Antes de que los *Gateways* VPN puedan crear túneles, primero deben autenticarse entre sí presentando uno de los siguientes tipos de credenciales:

- Certificados
- *Pre-shared secret*

Cada terminador de túnel comparte un certificado que contiene información que identifica al propio terminador y las credenciales utilizadas para crear el túnel VPN. Ambos elementos están firmados por la autoridad de certificación de confianza (CA). Check Point instala su propia CA interna que puede emitir certificados para todas las pasarelas de seguridad

gestionadas internamente. Además, *SmartConsole* y *Security Management Server* admiten el uso de CA externas.

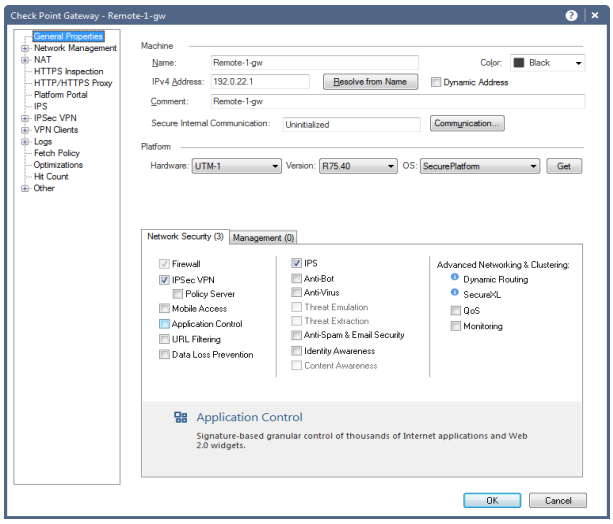
Si se necesita crear un túnel VPN con una puerta de enlace VPN administrada por un Servidor de administración de seguridad diferente (administrado externamente), a menudo es necesario utilizar *pre-shared secrets* para la autenticación.

Se puede configurar un *VPN Gateway* para enrutar el tráfico VPN en función de los dominios VPN o la configuración de enrutamiento del sistema operativo. En una VPN basada en dominio, el tráfico VPN se enruta según los dominios VPN definidos en *SmartConsole*.

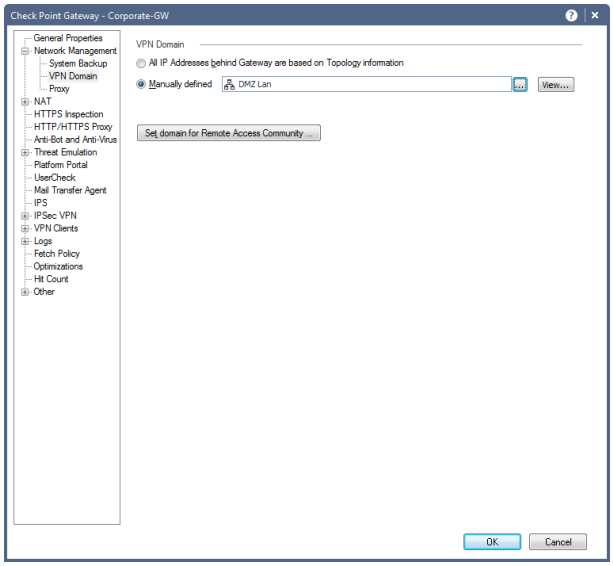
En algunas implementaciones avanzadas, existen configuraciones de enrutamiento específicas en el sistema operativo del *VPN Gateway*, como el enrutamiento dinámico. El tráfico VPN se puede configurar para que se enrute de acuerdo con estas configuraciones. Esto se conoce como VPN basadas en rutas. La puerta de enlace VPN utiliza una interfaz virtual llamada VPN Tunnel Interface (VTI), que envía el tráfico como si fuera una interfaz física. Las VTI de los terminadores de túneles en una comunidad VPN se conectan y pueden admitir protocolos de enrutamiento dinámico.

Para configurar una *VPN site-to-site* lo primero será definir las redes a y desde las que el tráfico debe ser encriptado.

- Habilitar el *blade* de IPSEC VPN en el objeto *Gateway*:



- Editar el objeto Gateway y definir el dominio de la VPN: Network Management ➔ VPN Domain

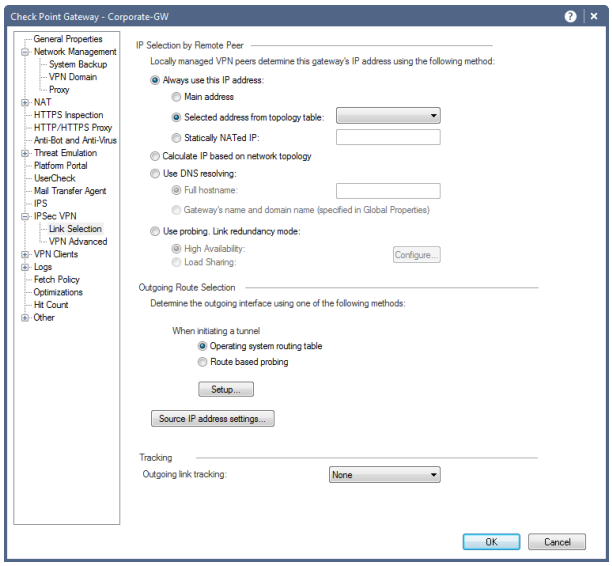


Si se selecciona la primera opción todas las direcciones IP que se encuentran tras el Gateway, según la topología establecida, pertenecen al Dominio VPN.

Si se escoge la segunda opción podemos definir de forma más específica que redes o conjunto de redes forman dicho Dominio VPN.

– Selección de enlace, editar el objeto Gateway y en el menú IPSEC VPN ➔ Link Selection definir qué interfaz se utiliza para el tráfico VPN entrante y saliente, así como la mejor ruta posible para el tráfico. El administrador puede elegir qué direcciones IP se utilizan para el tráfico VPN en cada Security Gateway:

  - Usar un sondeo para elegir enlaces según su disponibilidad.
  - Usar *Load Sharing* para la selección de enlaces y así distribuir el tráfico VPN a través de los enlaces disponibles.
  - Basado en el servicio para controlar el uso del ancho de banda.



En configurar una cierta dirección IP que siempre se usa las opciones son:

– Dirección principal: el túnel VPN se crea con la dirección IP principal del *Security Gateway*, especificada en el campo “Dirección IP” en la página “Propiedades generales” de *Security Gateway*.

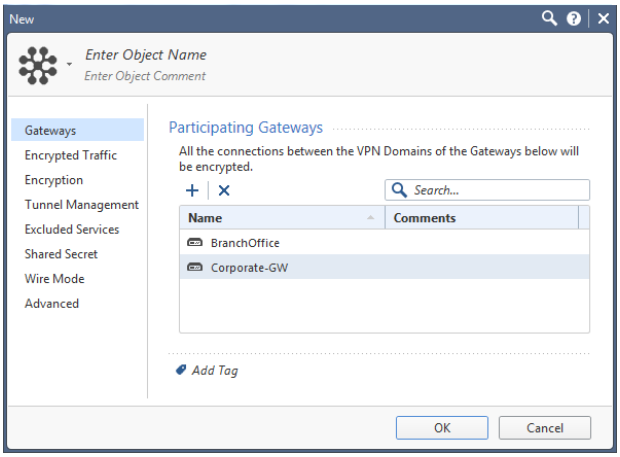
- Dirección seleccionada de la tabla de topología: el túnel VPN se crea utilizando una dirección IP seleccionada del menú desplegable que enumera las direcciones IP de la "Topología del Security Gateway".
- IP NAT estáticamente: el túnel VPN se crea utilizando una dirección IP de NAT. No es necesario que aparezca en la lista de topología.
- Calcular IP basada en la topología de red: El túnel VPN se crea utilizando una dirección IP de una interfaz externa en la puerta de enlace local. Selecciona la primera dirección IP en la lista de interfaces externas. Este método es mejor cuando la dirección IP principal de la puerta de enlace local es desconocida y las interfaces externas cambian con frecuencia.
- Usar *DNS Resolving*: Se usan con *Security Gateways* con asignación de IP dinámica (DAIP). En estos casos solo se puede iniciar utilizando la resolución DNS ya que la dirección IP no se puede conocer con anticipación. Si utiliza este método para una puerta de enlace de seguridad que no es DAIP, la dirección IP debe definirse en la pestaña de topología. Las opciones existentes son:
  - Nombre de host completo: nombre completo de dominio (FQDN).
  - Nombre del Security Gateway/Quantum Spark y nombre de dominio (especificados en propiedades globales): El nombre del Security Gateway/Quantum Spark se deriva de la página "*General Properties*" del Security Gateway/Quantum Spark y el nombre de dominio se deriva de la página "*Global Properties*".

Al utilizar sondeo en modo de redundancia: Cuando hay más de una dirección IP disponible en una puerta de enlace de seguridad para VPN, Link Selection puede emplear el método de prueba RDP para determinar qué enlace se usará. El método de prueba RDP se implementa utilizando un protocolo patentado que usa el puerto UDP 259. Este protocolo es propiedad de Check Point y funciona solo entre entidades de Check Point. Las direcciones IP que no desea sondear (es decir, direcciones IP internas) pueden eliminarse de la lista de direcciones IP que se probarán. Una vez que *Security Gateway/Quantum Spark* asigna la disponibilidad de los enlaces, se puede realizar una selección de enlaces por conexión de acuerdo con los siguientes modos de redundancia:

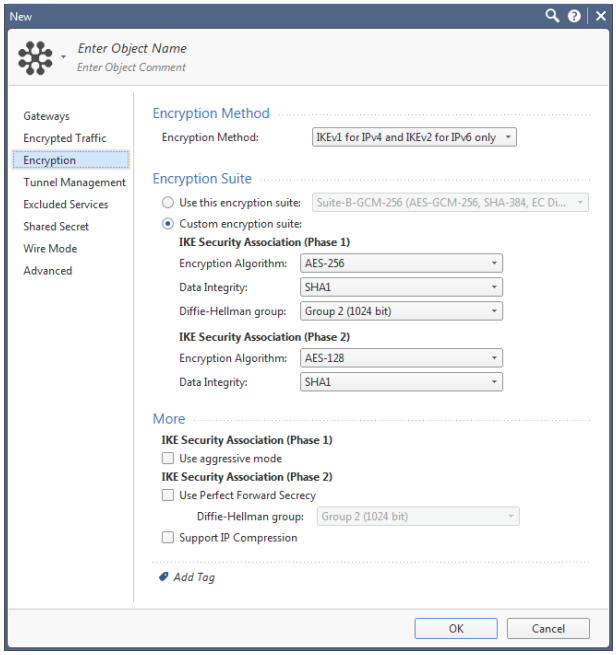
- Alta disponibilidad (configuración predeterminada): El túnel VPN usa la primera dirección IP para responder, o la dirección IP primaria si una IP primaria está configurada y activa. Si la dirección IP elegida deja de responder, la conexión pasa a otra dirección IP que responda.
- Compartición de carga (*Load Sharing*): El tráfico cifrado se distribuye entre todos los enlaces disponibles. Cada conexión nueva lista para el cifrado utiliza el siguiente enlace disponible en forma de turno rotativo. Cuando un enlace deja de estar disponible, todas sus conexiones se distribuyen entre los otros enlaces disponibles. La disponibilidad de un enlace se determina mediante el sondeo RDP.
- El otro extremo *VPN Gateway* responderá a la conexión enrutando el tráfico de respuesta a través de la misma ruta en la que se recibió, siempre que ese enlace esté disponible.

Para el tráfico saliente, existen diferentes métodos que se pueden usar para determinar qué ruta usar cuando se conecta con un par remoto.

- Tabla de enrutamiento del sistema operativo (configuración predeterminada): con este método, se consulta la tabla de enrutamiento para obtener la ruta disponible con la métrica más baja y la mejor coincidencia para el tráfico del túnel VPN.
- *Route based probing*: Este método también consulta la tabla de enrutamiento para obtener una ruta disponible con la métrica más baja y la mejor coincidencia. Sin embargo, antes de elegir una ruta, se prueba su disponibilidad mediante el sondeo RDP. A continuación, *Security Gateway/Quantum Spark* selecciona la ruta activa de mejor coincidencia (mayor longitud de prefijo) con la métrica más baja. Este método se recomienda cuando hay más de una interfaz externa.
- Crear una nueva Comunidad VPN: Añadir los terminadores de túneles que forman parte de esta comunidad VPN.

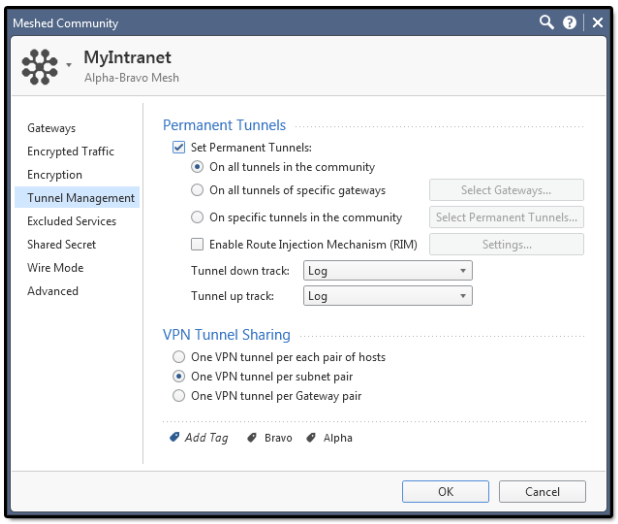


- Elegir el método de encriptación (IKEv1, IKEv2,…), además elegir el conjunto de algoritmos que se utilizarán en las SA tanto de la Fase 1 como de la Fase 2.



- Túneles VPN permanentes: Se mantienen constantemente activos por lo que es más fácil detectar problemas de conectividad. Los túneles permanentes solo se pueden establecer entre las puertas de enlace VPN de Check Point. Los túneles VPN permanentes se pueden configurar:

- En todos los túneles de la comunidad.
- En todos los túneles para puertas de enlace específicas.
- En túneles específicos en la comunidad.



Dado que los túneles permanentes se supervisan constantemente, si el túnel VPN no funciona, *SmartConsole* puede enviar un log, una alerta o una acción definida por el usuario. Un túnel VPN se controla enviando periódicamente paquetes de prueba. Si se reciben respuestas a los paquetes, se considera que el túnel VPN está activo. Si no, dentro de un período de tiempo determinado, el túnel VPN se considera inactivo.

9.2.2.1 VPN SITE TO SITE CON CERTIFICADO Y SECURITY GATEWAYS EXTERNOS

La configuración de una VPN entre *Security Gateways* externos (aquellos administradas por una consola de gestión diferente) tiene como peculiaridades:

- La configuración se realiza por separado en dos sistemas distintos.
- Todos los detalles deben ser acordados y coordinados entre los administradores. Los detalles, como la dirección IP o la topología del dominio VPN, no se pueden detectar automáticamente, el administrador debe proporcionarlos manualmente.
- Es probable que los miembros de las VPN usen diferentes Autoridades de Certificación (CA). Incluso si los Security Gateways utilizan la CA interna (ICA), sigue siendo una CA diferente.

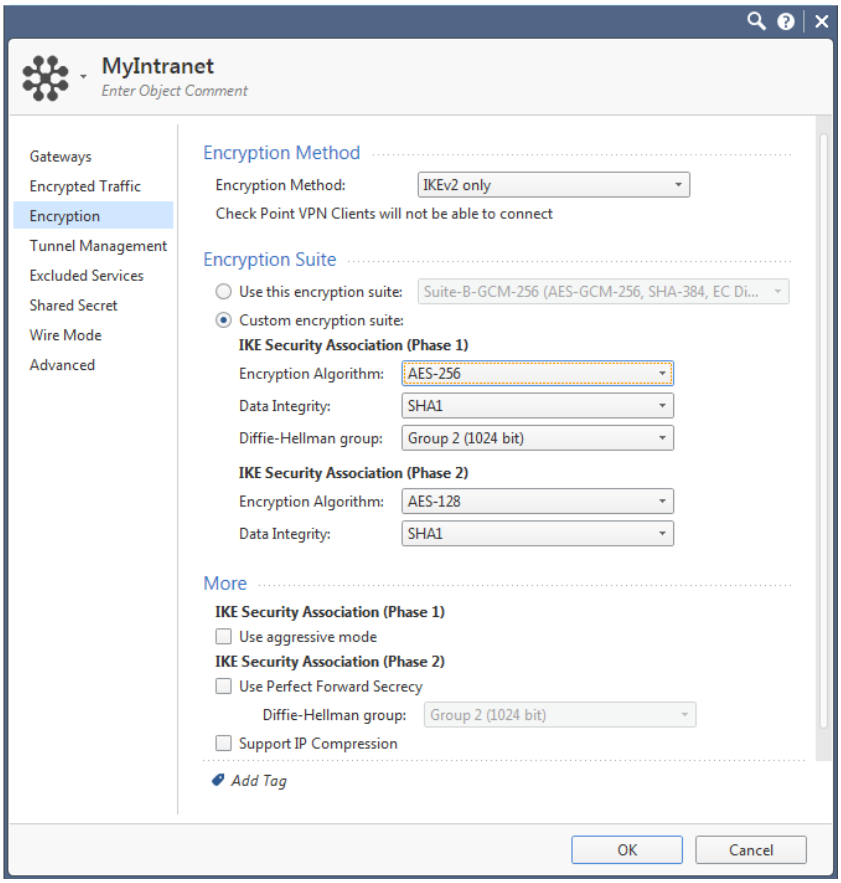
Para configurar VPN utilizando certificados, con *Security Gateways* externos como satélites en una comunidad VPN con topología de estrella:

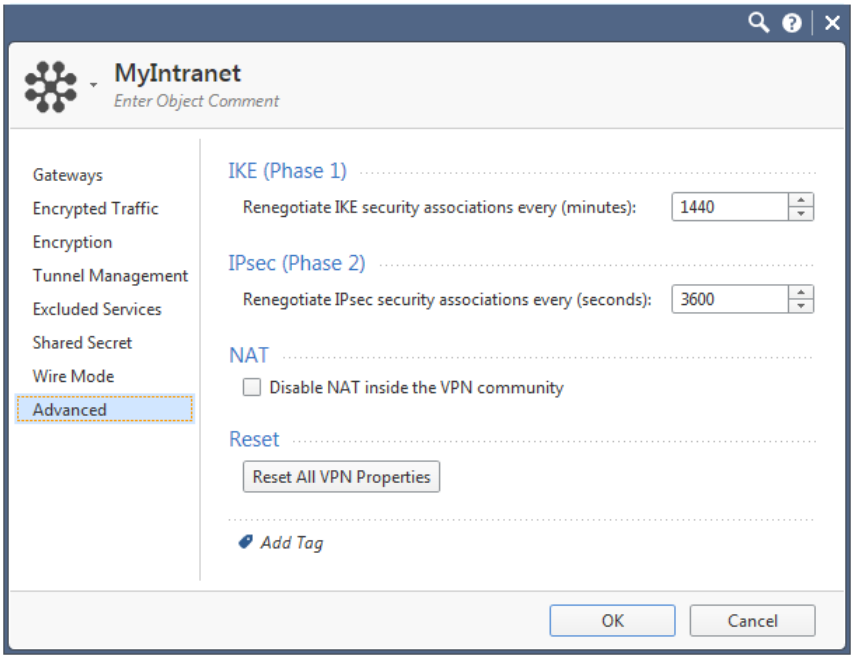
- Obtener el certificado de la CA que emitió para el “peer VPN Security Gateway”, del administrador. Si el “peer” está utilizando la ICA, puede obtener el certificado de CA mediante un navegador web:

  http: // <dirección IP del peer Security Gateway/Quantum Spark o Management Server>: 18264

- En SmartConsole, definir el objeto de CA para la CA que emitió el certificado para el “peer”.
- Definir la CA que emitirá los certificados para su lado si el Certificado emitido por ICA no es apropiado para el túnel VPN requerido.

- Es posible que tenga que exportar el certificado de CA y suministrarlo al administrador del "peer".
- Definir los objetos de red de los Security Gateways que se administran localmente. En particular, asegúrese de hacer lo siguiente:
    - En la página Propiedades generales del objeto Puerta de enlace de seguridad, seleccione VPN de IPsec.
    - En la página de Gestión de red, defina la Topología.
    - En la página Dominio de VPN, defina el Dominio de VPN. Si no contiene todas las direcciones IP detrás de *Security Gateway*, defina el dominio VPN manualmente definiendo un grupo o red de máquinas y configurándolas como el dominio VPN.
- Si el certificado ICA no es apropiado para este túnel VPN, en la página VPN de IPsec, genere un certificado de la CA correspondiente.
- Definir los objetos de red de las puertas de enlace de seguridad administradas externamente.
    - Si no es un Check Point Security Gateway, defina un dispositivo interoperable: en el Explorador de objetos, pulse New ➔ Network Object ➔ More ➔ Interoperable Device.
    - Si es una puerta de enlace de seguridad Check Point, defina una puerta de enlace VPN administrada externamente: En el Explorador de objetos, pulse en New ➔ Network Object ➔ Gateways and Servers ➔ More ➔ Externally Managed VPN Gateway.
- Establecer los diversos atributos del Security Gateway/Quantum Spark del peer. En particular, asegúrese de hacer lo siguiente:
    - Para un Check Point Security Gateway/Quantum Spark administrado externamente: en la página Propiedades generales del objeto Security Gateway, seleccione VPN de IPsec.
- Definir el dominio VPN utilizando la información del dominio VPN obtenida del otro administrador. Si el dominio VPN no contiene todas las direcciones IP detrás de Security Gateway, defina el dominio VPN manualmente definiendo un grupo o red de máquinas y configurándolas como el dominio VPN.
    - Para una Security Gateway/Quantum Spark de Check Point administrado externamente: en la página VPN de IPsec, defina los criterios de macheo. Especifique que el "peer" debe presentar un certificado firmado por su propia CA. Si es posible, aplique los detalles que aparecen en el certificado también.
- Definir la comunidad. Póngase de acuerdo con el administrador del mismo nivel sobre las distintas propiedades de IKE y configúrelas en la página Encriptación y en la página Avanzada del objeto de comunidad. Por ejemplo limitando al uso de IKEv2:





- Definir las puertas de acceso centrales de seguridad. Estos suelen ser los gestionados internamente. Si no se define ninguna otra comunidad para ellos, decida si va a combinar o no las pasarelas de seguridad centrales. Si ya están en una comunidad, no mezcle las puertas de enlace de seguridad centrales. En caso de una topología en estrella.
- Definir las pasarelas de seguridad satelital. Estos suelen ser los externos.

- Pulsar en Aceptar y publique los cambios.
- Definir las reglas de acceso relevantes en la Política de Seguridad.
- Agregar la Comunidad en la columna VPN, los servicios en la columna Servicios y Aplicaciones, la Acción deseada y la opción de Seguimiento correspondiente.
- Instalar la Política de Control de Acceso.

9.2.3 VPN DE ACCESO REMOTO

Una implementación de VPN de acceso remoto maneja la comunicación segura entre los recursos corporativos internos y los usuarios remotos que usan túneles VPN. Si los usuarios acceden de forma remota a información confidencial desde diferentes ubicaciones y dispositivos, los administradores del sistema deben poder proporcionar acceso seguro a esa información.

Nota: la computadora o dispositivo remoto requiere un software VPN especial, para conectarse al túnel VPN y encriptar la comunicación con la puerta de enlace VPN.

Las soluciones VPN de Check Point para acceso remoto usan protocolos de encriptación IPsec y SSL para crear conexiones seguras entre la computadora o dispositivo remoto y el *VPN Gateway*.

EL *Gateway* y el cliente remoto deben establecer confianza para crear un túnel VPN. Esto se hace cuando el *Gateway* verifica la identidad del usuario y el cliente remoto verifica la identidad del *Gateway*. Los usuarios remotos se autentican con certificados digitales o *pre-shared secret*.

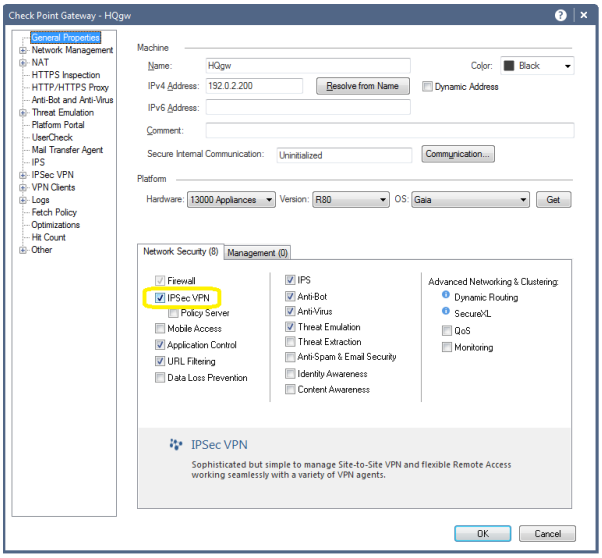
Acceso remoto basado con cliente: los usuarios instalan una aplicación o cliente de software en sus computadoras y dispositivos de punto final. El cliente proporciona acceso remoto seguro a la mayoría de los tipos de recursos corporativos de acuerdo con los privilegios de acceso del usuario.

Acceso remoto sin cliente: los usuarios se autentican con un navegador de Internet y usan conexiones HTTPS seguras. Las soluciones sin cliente a menudo brindan acceso a recursos corporativos basados en la web.

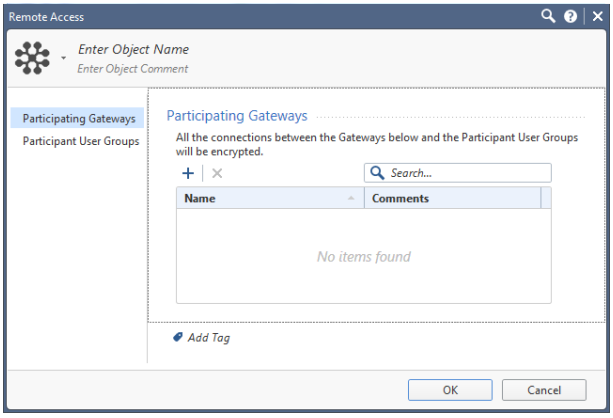
Existe un modo de configuración, *Office Mode* que permite a un *Security Gateway/Quantum Spark* asignar a un cliente remoto una dirección IP. La asignación tiene lugar una vez que el usuario se conecta y se autentica. Después de que el usuario se autentica, la puerta de enlace VPN asigna una dirección IP al cliente remoto. La puerta de enlace VPN encapsula los paquetes IP con una dirección IP disponible de la red interna.

Para configurar una VPN de acceso remoto:

- Habilitar el *Blade* de IPSEC VPN en el objeto *Gateway*:

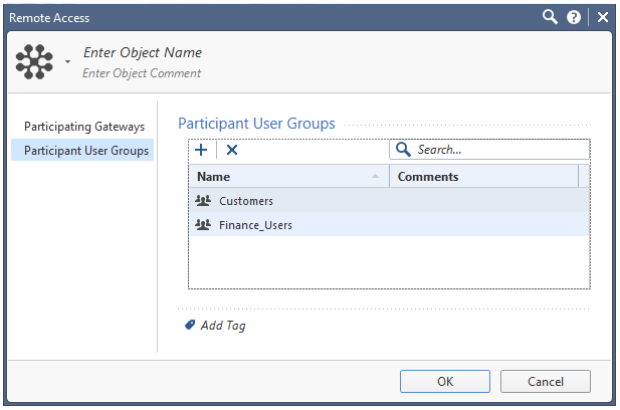


– Crear una nueva comunidad VPN de Acceso Remoto:

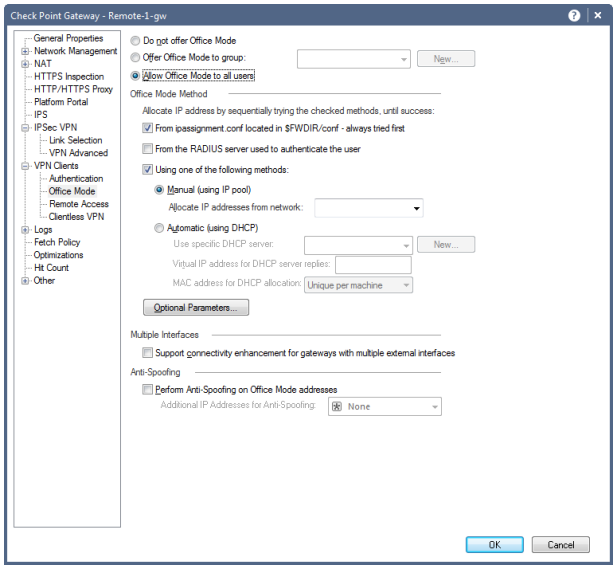


– Añadir el Gateway que haga de terminador de túneles para las VPN de Acceso Remoto.

– Añadir el o los grupos de usuarios que van a conectarse mediante la VPN de Acceso Remoto.



– Una vez creada la comunidad VPN, editar el objeto Gateway correspondiente y en la pestaña de “VPN Clients”, elegir “Office Mode”.



El modo oficina permite a un *Security Gateway/Quantum Spark* asignar a un cliente remoto una dirección IP. La asignación tiene lugar una vez que el usuario se conecta y se autentica. La dirección puede tomarse desde un grupo de direcciones IP generales, o desde un grupo de direcciones IP especificado por grupo de usuarios. La dirección se puede especificar por usuario o a través de un servidor DHCP. Se pueden asignar utilizando uno de los siguientes métodos:

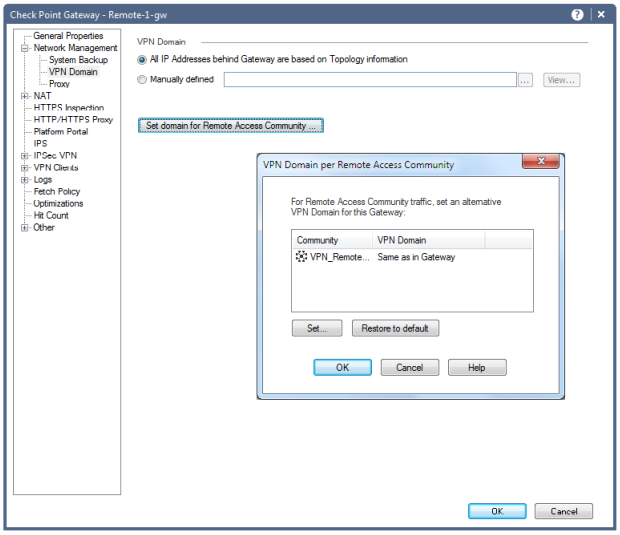
- IP Pool: El administrador del sistema designa un rango de direcciones IP que se utilizarán para las máquinas de clientes remotos. Cada cliente que solicita conectarse en modo *Office* recibe una dirección IP única de dicho *pool*. Las direcciones IP del grupo de IP pueden reservarse y asignarse a usuarios remotos en función de su dirección IP de origen.
- servidor DHCP: Se puede usar un servidor DHCP para asignar direcciones. Cuando un usuario remoto se conecta, el *Security Gateway/Quantum Spark* solicita al servidor DHCP que asigne al usuario una dirección IP desde un rango de direcciones IP designadas para los usuarios del Modo Oficina.

Además, un servidor RADIUS se puede usar para autenticar usuarios remotos. Cuando un usuario remoto se conecta a un *Security Gateway*, el nombre de usuario y la contraseña se pasan al servidor RADIUS, que verifica que la información sea correcta y autentica al usuario. El servidor RADIUS también se puede configurar para asignar direcciones IP.

Normalmente, el enrutamiento se realiza antes del cifrado en VPN. En algunos escenarios complejos de *Office Mode*, donde *Security Gateway/Quantum Spark* puede tener varias interfaces externas, esto podría causar un problema. En estos escenarios, los paquetes destinados a la dirección IP virtual de un usuario remoto se marcarán como paquetes que se deben enrutar a través de una interfaz externa de *Security Gateway*. Solo después de que se toma la decisión de enrutamiento inicial, los paquetes pasan por una encapsulación IPsec. Después de la encapsulación, la dirección IP de destino de estos paquetes cambia a la dirección IP original del cliente. La ruta de enrutamiento que debería haberse seleccionado para el paquete encapsulado podría ser a través de una interfaz externa diferente a la del paquete original (ya que la dirección IP de destino cambió), en cuyo caso se produce un error de

enrutamiento. *Office Mode* tiene la capacidad de asegurarse de que todos los paquetes de modo de *Office* se enruten una vez que están encapsulados.

- Después, editar el objeto Gateway y definir el domino VPN: Network Management ➔ VPN Domain ➔ Set domain for Remote Access Community



- Configurar las *Access Rules* en la política de seguridad correspondiente a la VPN, para permitir que los usuarios de la comunidad VPN de acceso remoto accedan a la LAN.

9.2.3.1 VPN DE ACCESO REMOTO CON CERTIFICADOS

Check Point VPN le permite definir varios certificados para cada usuario. Esto permite a los usuarios conectarse desde diferentes dispositivos sin la necesidad de copiar o mover certificados de un dispositivo a otro. Los usuarios también pueden conectarse desde diferentes dispositivos al mismo tiempo.

La autoridad de certificación interna (ICA) de Check Point ofrece dos formas de crear y transferir certificados a usuarios remotos:

1. El administrador genera un certificado en el *Security Management Server* para el usuario remoto, lo guarda en cualquier medio extraíble y lo transfiere al cliente "fuera de banda".

2. El administrador inicia el proceso de certificado en el *Security Management Server* y recibe una clave de registro. El administrador transfiere la clave de registro al usuario "fuera de banda". El cliente establece una conexión SSL con la ICA (mediante el protocolo CMC) y completa el proceso de generación de certificados con la clave de registro. De este modo:

   - Las claves privadas se generan en el cliente.
   - El certificado creado se puede almacenar como un archivo en el disco duro de la máquina, en un dispositivo de almacenamiento CAPI o en un token de hardware.

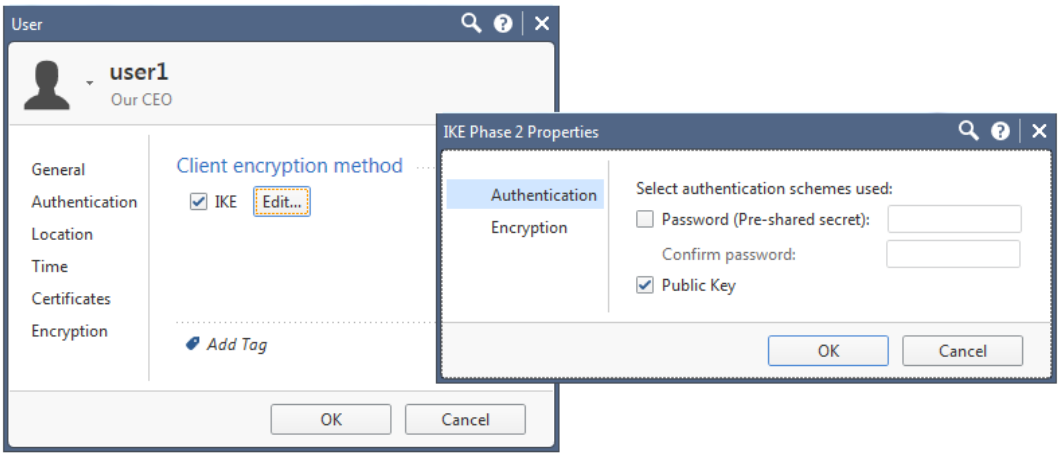
Este método es especialmente adecuado para usuarios remotos espaciados geográficamente.

Hay dos procedimientos básicos para suministrar certificados VPN de acceso remoto a los usuarios.

1. Enviando un archivo P12:
    - El administrador crea un archivo de certificado p12 y lo envía a los usuarios.
    - El usuario guarda el archivo p12 en el dispositivo y especifica el certificado utilizando un cliente VPN remoto.
    - Los usuarios se autentican ingresando una contraseña de certificado al iniciar una conexión VPN de acceso remoto.
2. Utilizando una clave de registro:
    - El administrador crea una clave de registro y la envía al usuario.
    - El usuario inscribe el certificado ingresando la clave de registro en un cliente VPN de acceso remoto. El usuario puede, opcionalmente, guardar el archivo p12 en el dispositivo. El usuario debe hacer esto en un período de tiempo definido por el administrador.
    - Los usuarios finales se autentican utilizando este certificado. También se puede requerir una contraseña de acuerdo con la configuración de la política de seguridad. Si el usuario guarda el archivo p12 en el dispositivo, siempre es necesaria una contraseña.

Para habilitar un certificado de usuario:

1. En *SmartConsole*, ir a Ojects y pulsar en *Users* ➔ *Users*.
2. Crear un nuevo usuario o editaar uno existente.
3. En la ventana de propiedades del usuario, pulsar en Encryption y Editar para abrir la ventana de propiedades de IKE Phase 2.

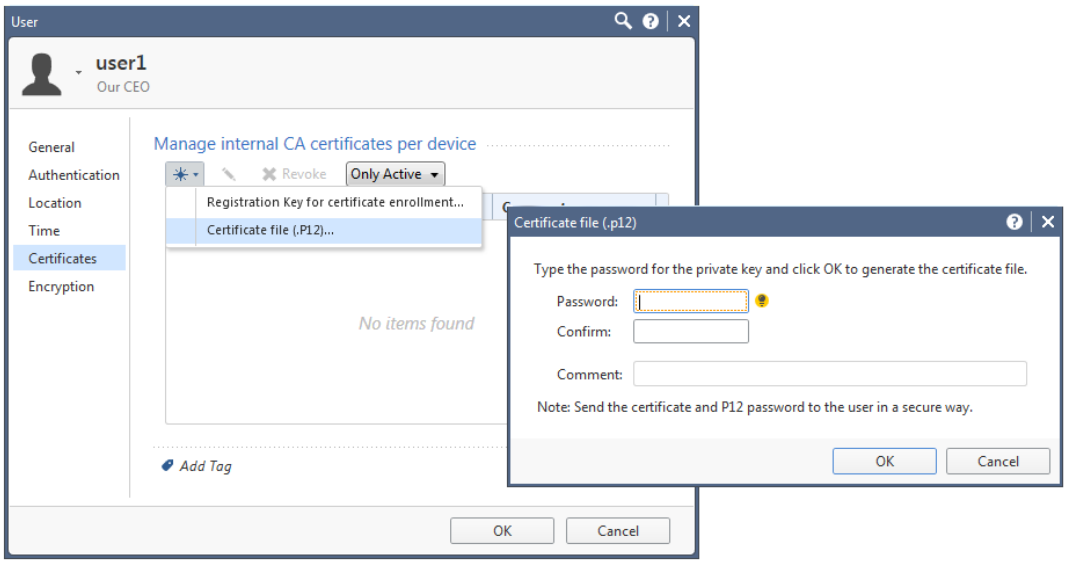


4. Pulsar en “Authentication” y asegurarse que la clave pública está seleccionada.
5. Pulsamos en OK y publicamos los cambios.

Después de crear un certificado de usuario, debe hacer que este certificado esté disponible para los usuarios de acceso remoto. Utilizar este procedimiento para crear un certificado p12.

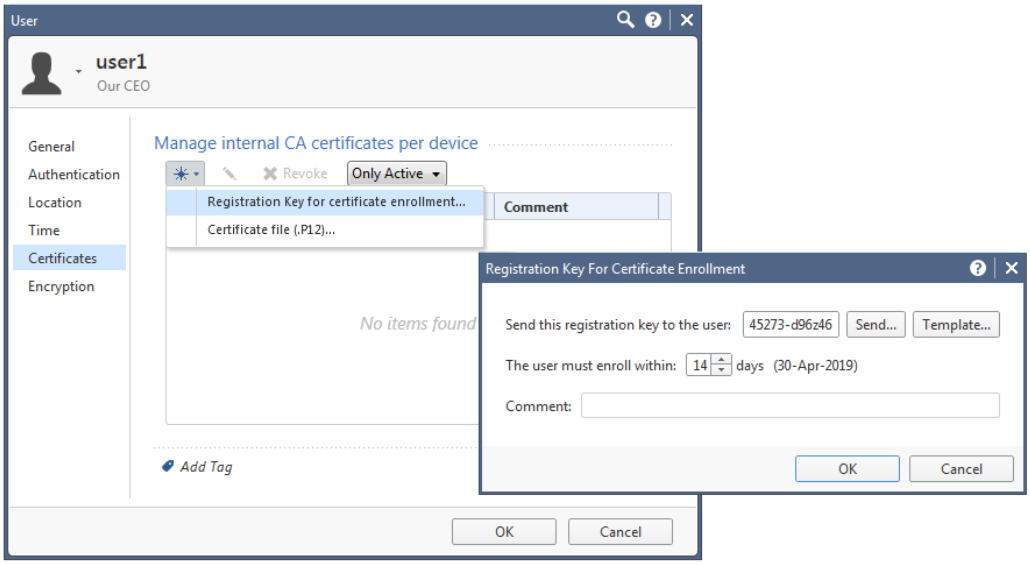
Para crear un archivo de certificado p12 para usuarios de VPN de acceso remoto:

1. Crear el certificado de usuario.
2. En la ventana “User properties”, en el árbol de navegación, haga clic en Certificados.
3. En la página Certificados, haga clic en Nuevo.
4. Seleccionar Archivo de certificado (.p12).
5. En la ventana Archivo de certificado (.P12), ingrese y confirme la contraseña del certificado.
6. Haga clic en Aceptar e ingrese una ruta para guardar el archivo p12.
7. El nuevo certificado se muestra en el certificado. El estado se establece en Válido.
8. Haga clic en Aceptar.
9. Envíe el archivo .p12 al usuario final por correo electrónico seguro u otro medio seguro.



En el caso de que usemos “certificate registration key” los pasos 1 al 3 serian iguales:

- Seleccionar Clave de registro para la inscripción del certificado.
- En la ventana Clave de registro para inscripción de certificado, seleccione el número de días antes de que caduque el certificado.
- Pulsar en el botón de correo electrónico para enviar la clave de registro al usuario.
- Pulsar en Aceptar.



El uso de PKI de terceros implica la creación de un certificado para el usuario y también un certificado para Security Gateway.

Puede utilizar una autoridad de certificación OPSEC PKI de terceros que admita los estándares PKCS # 12, CAPI o Entrust para emitir certificados para los *Gateways* de seguridad y los usuarios. *Security Gateway/Quantum Spark* debe confiar en la CA y tener un certificado emitido por la CA.

El nombre de usuario en la base de datos interna debe ser el DN completo que aparece en el certificado o simplemente el nombre que aparece en la parte CN del certificado. Por ejemplo, si el DN que aparece en el certificado es:

CN = John, OU = Finanzas, O = Widget Enterprises, C = US

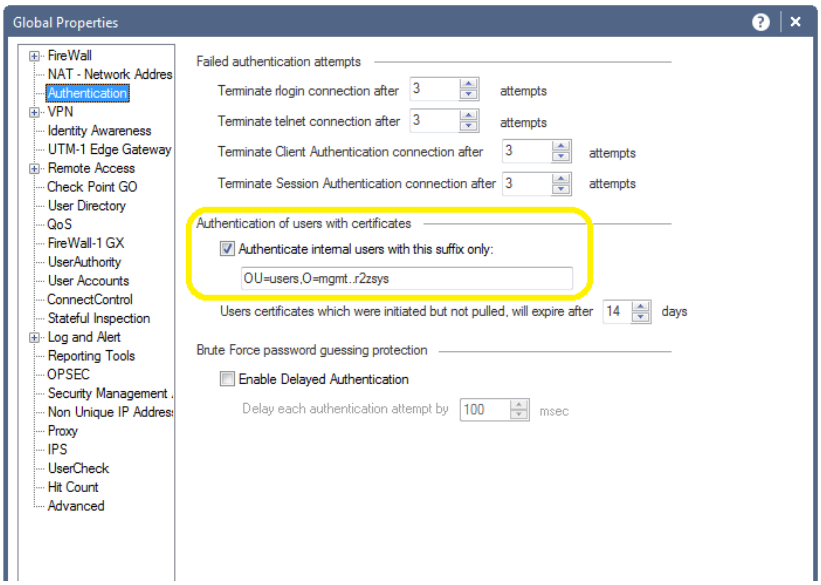
El nombre del usuario en la base de datos interna pueden ser: John

CN = John, OU = Finanzas, O = Widget Enterprises, C = US

Para utilizar una solución PKI de terceros:

- En *SmartConsole*, en la barra de objetos, pulse en *Usuarios* ➔ *Usuarios*.
- Crear un nuevo usuario o edite un usuario existente. Se abrirá la ventana Propiedades del usuario.
- En el árbol de navegación, pulse en Cifrado y en Editar. Se abrirá la ventana Propiedades de IKE Fase 2.
- Pulsar en la pestaña Autenticación y seleccione Clave pública.
- Definir la Autoridad de certificación de terceros como un objeto en *SmartDashboard*.
- Opcional: genere un certificado para su *Security Gateway/Quantum Spark* desde la CA de terceros.
- Genere un certificado para el usuario remoto desde la CA de terceros.
- Transfiera el certificado al usuario.

– En la ventana *Propiedades globales* ➔ *Autenticación*, agregue o deshabilite la coincidencia de sufijos.



Para los usuarios con certificados, es posible especificar que solo se aceptan certificados con un sufijo específico en su DN. Esta función está habilitada de forma predeterminada y solo es necesaria si:

– Los usuarios se definen en la base de datos interna, y

– Los nombres de usuario no son el DN completo.

Todos los DN de los certificados se comparan con este sufijo.

9.2.4 VPN TUNNEL SHARING

Proporciona una mayor interoperabilidad y escalabilidad al controlar la cantidad de túneles VPN creados entre los *VPN Gateways* similares. La configuración de la compartición de túneles VPN puede establecerse tanto en la comunidad VPN como en el objeto *Security Gateway*:

– Un túnel VPN por cada par de hosts: se crea un túnel VPN para cada sesión iniciada entre cada par de hosts.

– Un túnel VPN por cada par de subredes: una vez que se haya abierto un túnel VPN entre dos subredes, las sesiones subsiguientes entre las mismas subredes compartirán el mismo túnel VPN. Esta es la configuración predeterminada y cumple con el estándar de la industria IPsec.

– Un par de túneles VPN por *Gateway*: se crea un túnel VPN entre *VPN Gateways* para todos los *hosts* que hay detrás.

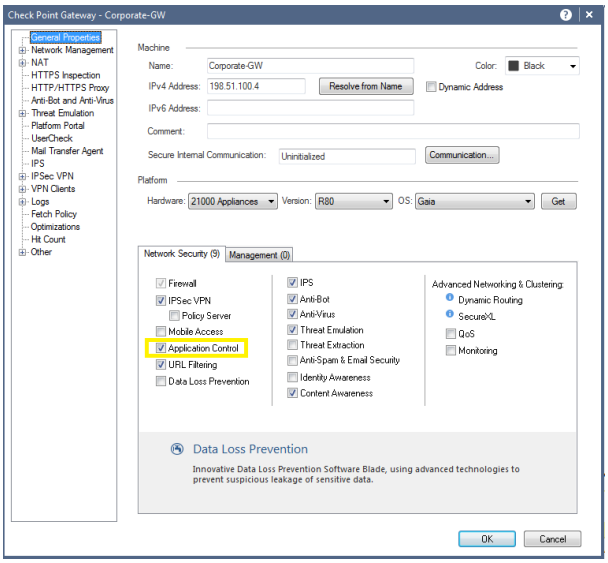
En caso de conflicto entre las propiedades del túnel de una comunidad VPN y un objeto *Security Gateway/Quantum Spark* que es miembro de esa misma comunidad, se sigue la configuración más restrictiva.

9.3 IDENTIFICACIÓN DE LA APLICACIÓN

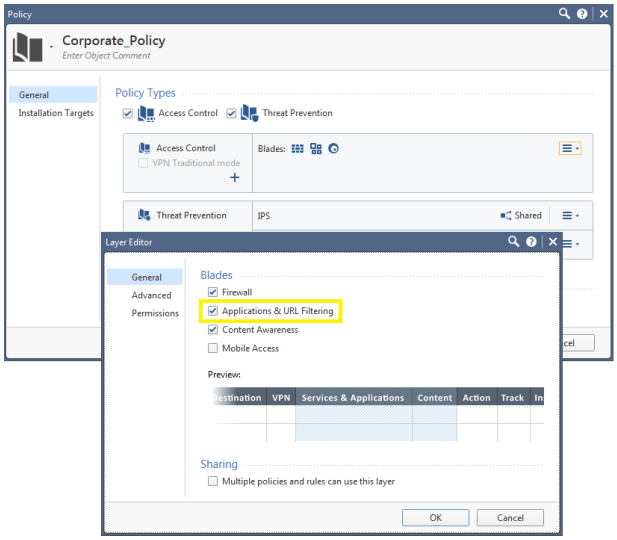
La identificación de aplicaciones permite que las Políticas de seguridad de aplicaciones identifiquen, permitan, bloquen o limiten el uso (en función del ancho de banda y/o tiempo) de aplicaciones y *widgets* de redes sociales, independientemente del puerto, protocolo o técnica evasiva utilizada. En combinación con *Identity Awareness*, se pueden crear definiciones de políticas detalladas.

AppWiki es una librería de aplicaciones que tiene registradas más de 7700 aplicaciones y 255.000 widgets de redes sociales, mensajería instantánea, anonimizadores, VoIP, SCADA, etc. Las aplicaciones son clasificadas en categorías, basadas en criterios como tipo de aplicación, potencial riesgo de seguridad, uso de recursos, limitación de la productividad. AppWiki es actualizada continuamente: http://appwiki.checkpoint.com/appwiki/applications.htm. Para su configuración:

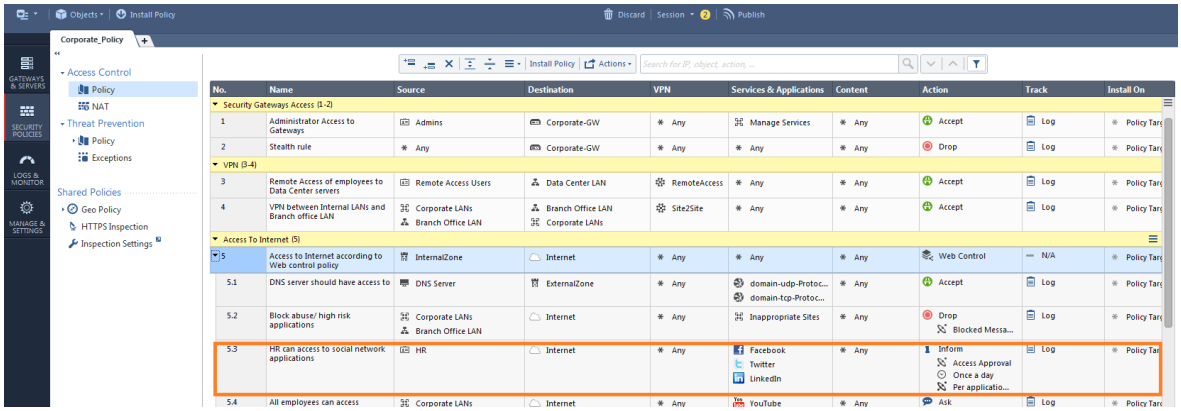
- Lo primero es habilitar el *Software Blade* de "Application Control" en el *Security Gateway/Quantum Spark* correspondiente:



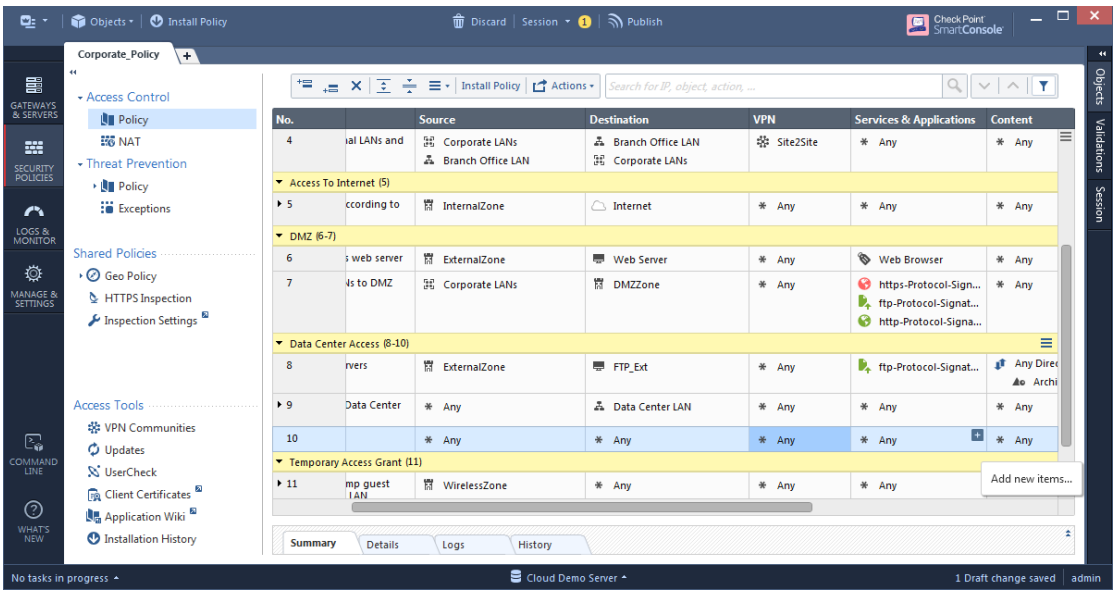
- El siguiente paso es habilitar el *Software Blade* de "Application Control" en la capa de la política de seguridad oportuna:



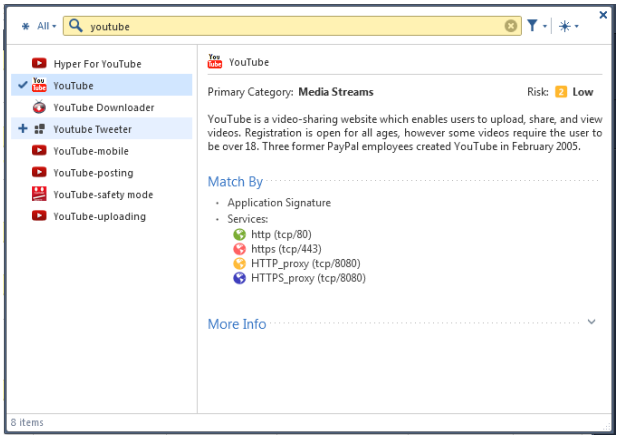
– Para agregar una aplicación a una regla ir a la Política de control de acceso, a la capa dónde acabamos de habilitar la funcionalidad:



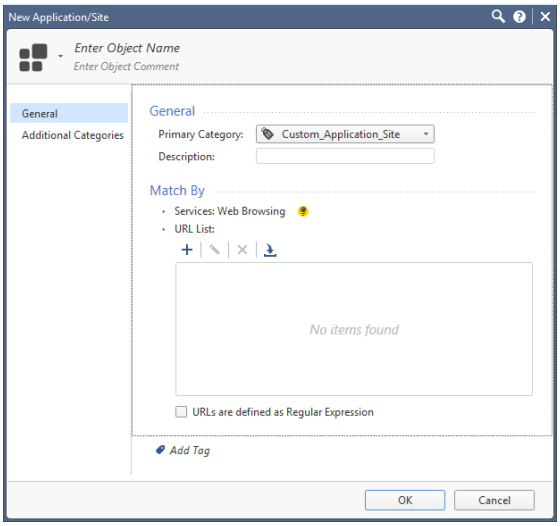
– En una regla existente o nueva, pulse con el botón derecho en la columna “Services & Applications” y seleccione “Agregar nuevos elementos”.



– Se abre la ventana del visor de aplicaciones.



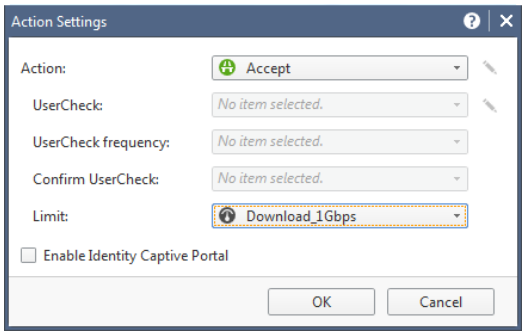
- Busque filtrando por aplicaciones.
- Pulsar en el signo “+” junto a los que desea agregar.
- Para crear una nueva aplicación. Pulsar en New ➔ Custom Applications / Sites



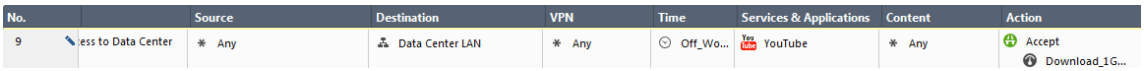
- Introducir el nombre para el objeto.
- Introducir una o más URL.
- Si se utiliza una expresión regular en la URL, es necesario hacer pulsar en “URLs are defined as Regular Expression”.
- Pulsar en Aceptar.

Si no se desea bloquear una aplicación o categoría, existen diferentes formas de establecer límites para el acceso de los usuarios a las aplicaciones:

- Agregar un objeto Límite a una regla para limitar el ancho de banda permitido para dicha regla. Botón derecho en la columna “Action”, seleccionar la opción “More”. Y establecer el objeto “Limit”:



– Agregar uno o más objetos "Time" a una regla para que se active solo durante los tiempos especificados.



Nota: La columna "Hora" no se muestra de forma predeterminada en la tabla "Base de reglas". Para verlo, pulse derecho en el encabezado de la tabla y seleccione "Time".

9.4 FILTRADO DE URL

El *Software Blade* de *URL Filtering* protege a los usuarios y organizaciones mediante la restricción de acceso a una lista de sitios y contenidos potencialmente peligrosos, bloqueando la navegación Web hacia URLs categorizadas en clasificaciones diferentes, actualizadas continuamente de forma automática. Las plantillas de política predefinidas permiten un despliegue usando categorías por contenido. Todos los perfiles son actualizados continuamente mediante el servicio de actualización de software de Check Point.

Los beneficios fundamentales son los siguientes:

– Protege al usuario del contenido inapropiado o peligroso.

– Protege a la organización del uso inapropiado o ilegal de los recursos de red.

– Política corporativa personalizable.

– Automatizado para requerir mantenimiento mínimo.

– Activación instantánea.

La combinación de *URL Filtering, Application Control* e *Identity Awareness*, permite unificar el control de acceso a sitios web con el control de aplicaciones web y *widgets* para una mayor granularidad. Permitiendo definir reglas para permitir, bloquear o limitar acceso (basado en el tiempo y/o ancho de banda) de aplicaciones, categorías de URL, o incluso a nivel de riesgo. Pudiendo aplicar dichas reglas de seguridad a grupos o usuarios concretos.

La solución unificada de Check Point de Filtrado de URL y Control de Aplicaciones proporcionan:

– Una Base de reglas comunes para simplificar la creación de políticas conjuntas en todas las categorías, tanto para sitios web y aplicaciones.

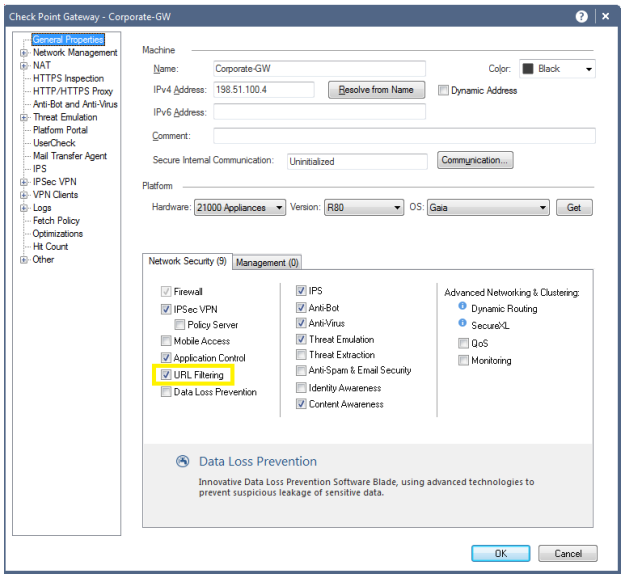
– Una consola de gestión para facilitar la gestión.

– Un sistema de información para mejorar la visibilidad en los eventos web.

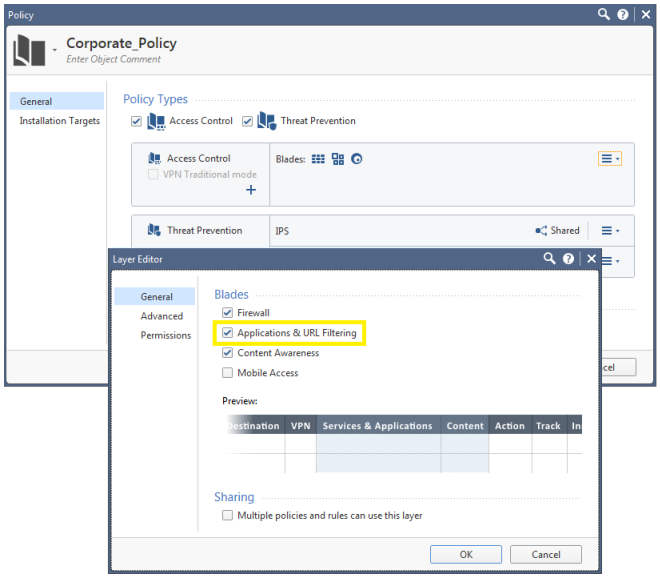
- Listas blancas y listas negras.

Para configurar el filtrado de URL:

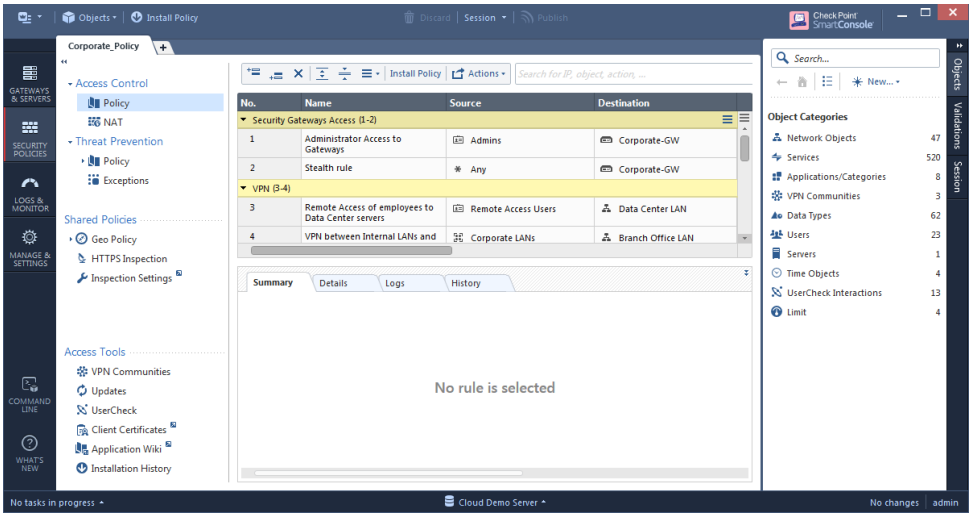
- Lo primero es habilitar el Software Blade de URL Filtering en el Security Gateway/Quantum Spark correspondiente:



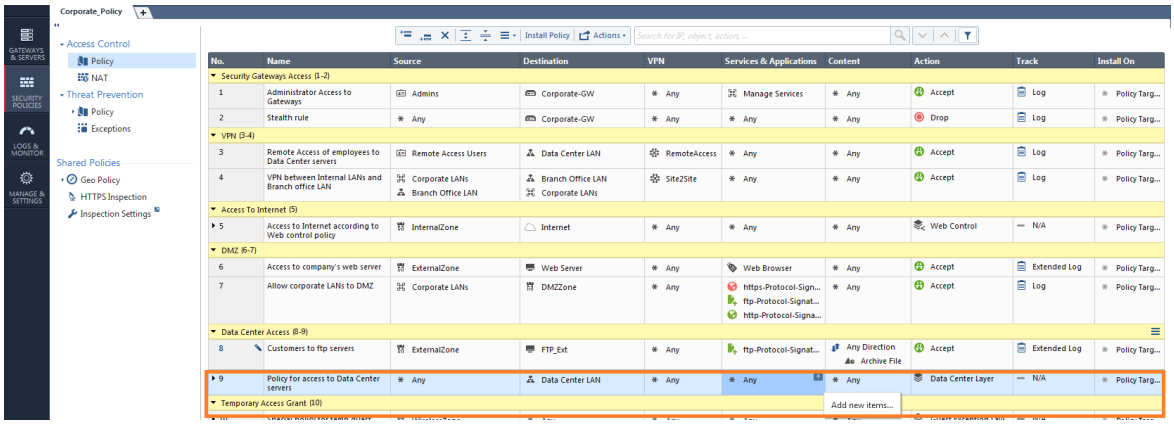
- El siguiente paso es habilitar el Software Blade de URL Filtering en la capa de la política de seguridad oportuna:



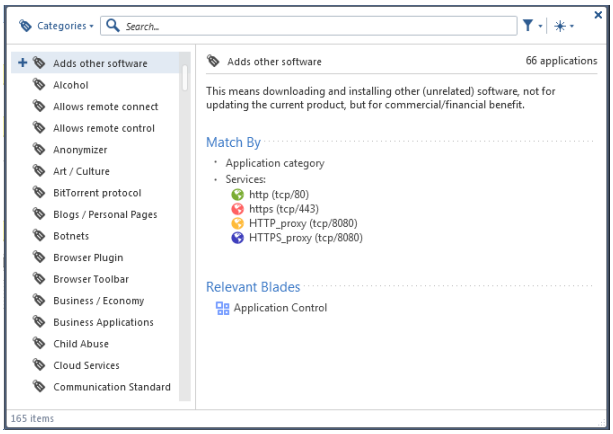
- Ir a la Política de control de acceso, a la capa dónde acabamos de habilitar la funcionalidad:



– En una regla de seguridad existente o nueva, pulse con el botón derecho en la celda "Servicios y aplicaciones" y seleccione "Agregar nuevos elementos".



– Se abre la ventana del visor de aplicaciones. Centrándonos en las categorías:



Nota: las categorías se combinan con sus servicios recomendados, donde cada servicio se ejecuta en un puerto específico, como por ejemplo los servicios de exploración web de control de aplicaciones predeterminados: http, https, HTTP_proxy y HTTPS_proxy.

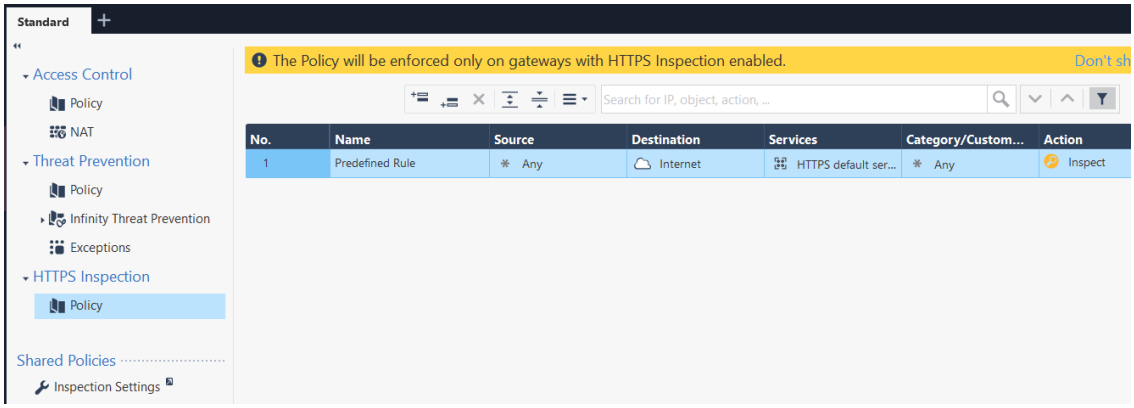
9.5 INSPECCIÓN HTTPS

Es posible analizar y asegurar el tráfico cifrado SSL que pasa a través del *Gateway*. Cuando el tráfico pasa a través de este, el *Gateway* descifra el tráfico con la clave pública del remitente, inspecciona y protege, y a continuación, vuelve a cifrar, enviando el contenido recién cifrado al receptor.

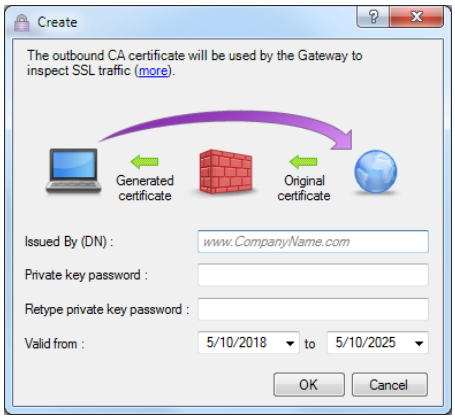
Se pueden definir excepciones para la inspección SSL para proteger la privacidad de los usuarios y cumplir con las políticas corporativas. Parte del contenido encriptado que pasa a través del *Gateway* no debería ser inspeccionado, pudiendo conseguirlo con una simple definición de política del administrador.

Para configurar la inspección HTTPS:

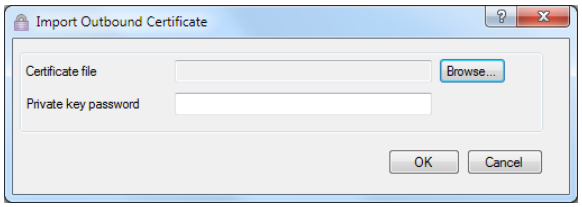
- Editar el objeto *Gateway*, seleccionar en el menú, la opción "HTTPS Inspection"



- Crear o importar un certificado de una CA externa. Para crear un certificado firmado por nuestra CA Interna:

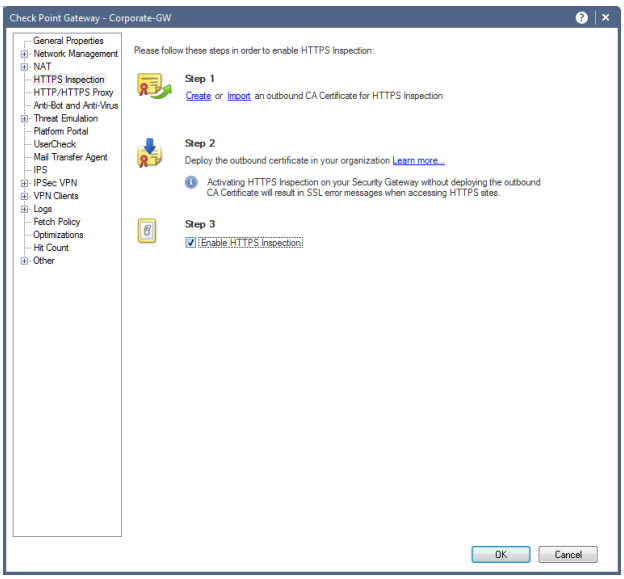


- Establecer el nombre del certificado y la clave privada, además de definir el rango de tiempo de validez del mismo. Importar un certificado:

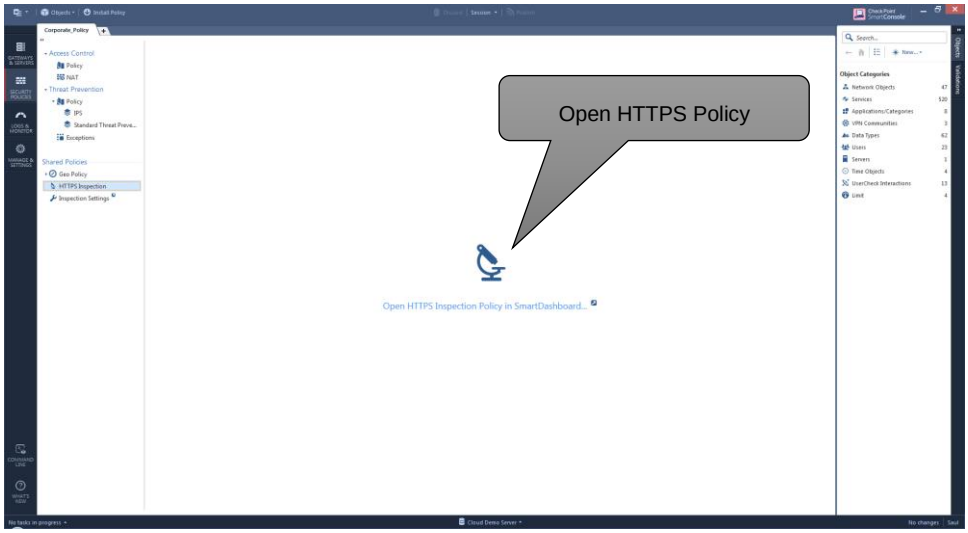


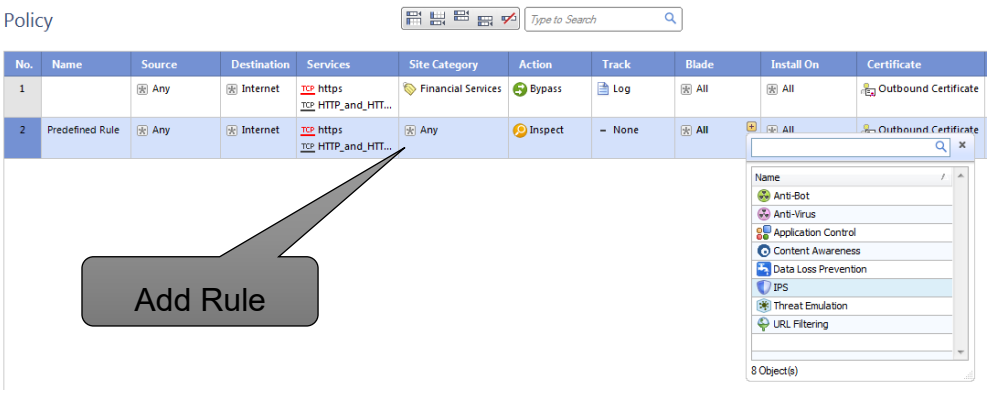
- Seleccionar el certificado e introducir la clave privada.

- Exportar el certificado a las máquinas necesarias.
- Activar *HTTPS Inspection*.



- Crear las Políticas de seguridad relacionadas con “HTTPS Inspection”. Dentro del menú de Políticas de seguridad, seleccionar “HTTPS Inspection”:

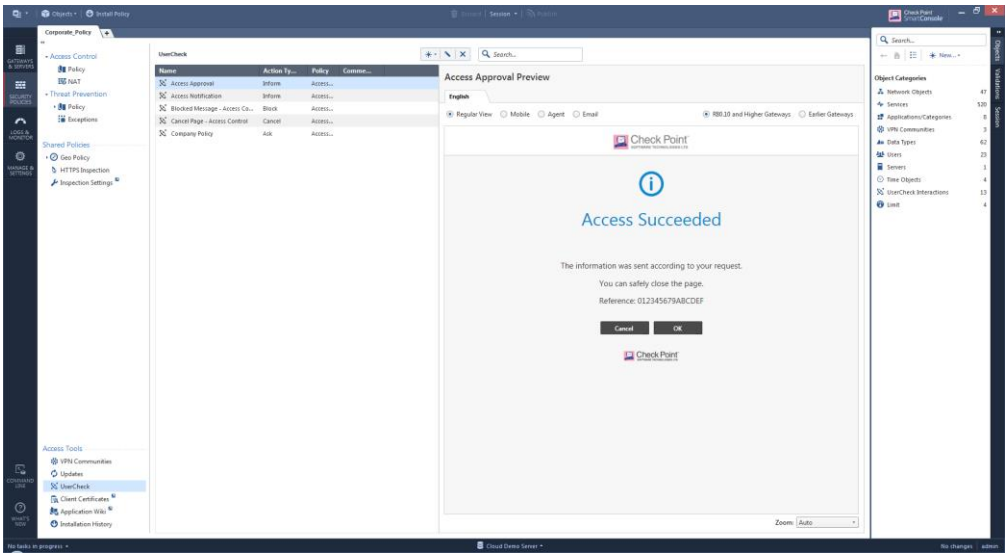




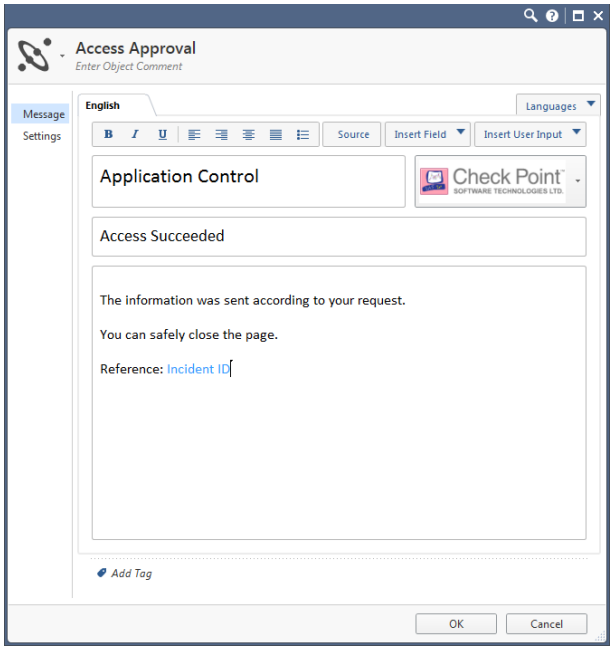
9.6 USERCHECK

La tecnología *UserCheck* informa al usuario en tiempo real acerca de sus limitaciones de acceso a las aplicaciones y informando sobre el riesgo de acceso a redes públicas y las políticas de uso de la organización. Además de definir una política para permitir o bloquear aplicaciones específicas, las organizaciones pueden permitir "decidir" al usuario sobre el uso de una aplicación, preguntando si es para un uso personal o corporativo. Para configurar *UserCheck*:

- El primer paso es definir la página web que se le mostrará al usuario: *Security Policies ➔ Access Tools ➔ UserCheck.*

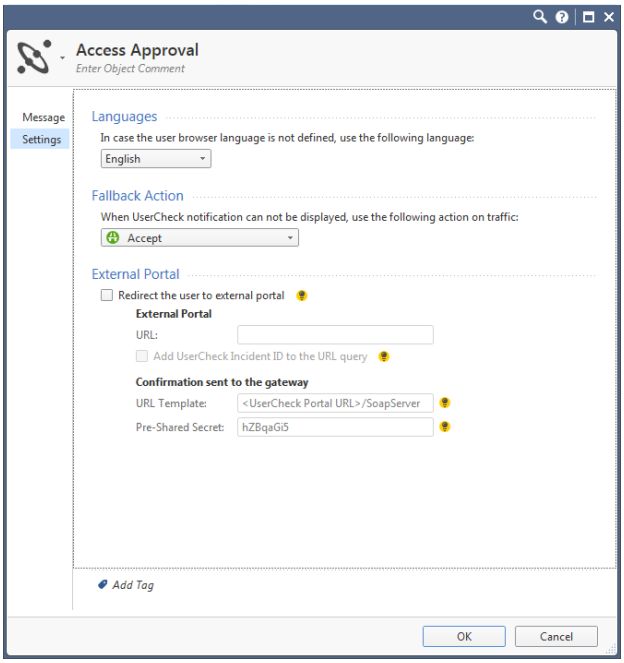


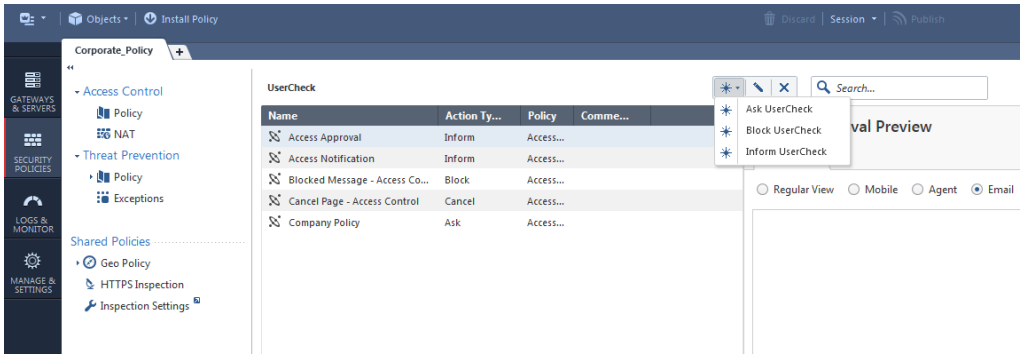
- Eligiendo una de la predefinidas y modificando lo que se considere necesario: *Mensaje prefinido ➔ Editar.*



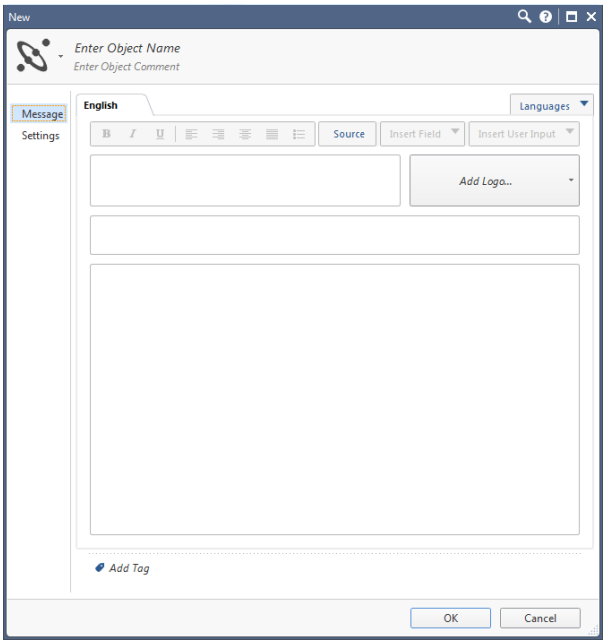
- Podemos no sólo modificar el mensaje y el logo, sino también modificar otros parámetros como por ejemplo, en caso de que no se pueda mostrar el mensaje qué acción tomar o redirigir al usuario a un portal externo.

– Otra opción es crear nuestro propio mensaje para mostrar al usuario.

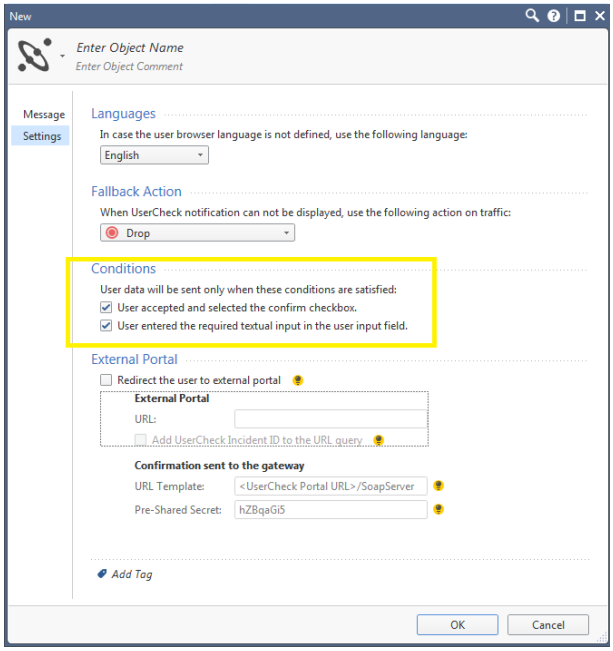




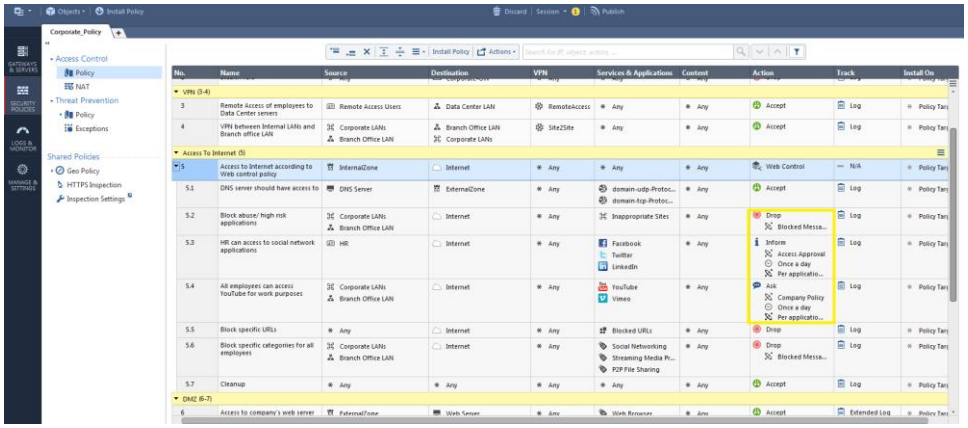
– Crear un mensaje para el usuario desde cero:



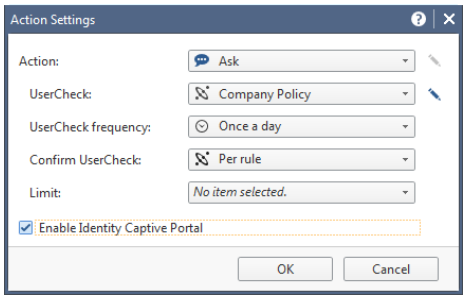
- En caso de que sea necesario una justificación por parte del usuario, puede ser necesario la siguiente configuración. Si es necesario que el usuario acepte y confirme y si además es necesario que introduzca una justificación para que se permita el tráfico.



- Una vez creado el mensaje a mostrar al usuario, es necesario fijar que se muestre dicho mensaje al usuario en la correspondiente regla de seguridad: Botón derecho en la columna *Action* ➔ *More* y seleccionar las distintas opciones.



- Seleccionar la frecuencia a la que se mostrará el mensaje al usuario y si se mostrará cada vez que se machea la propia regla se seguridad, por aplicación, por categoría o por tipo de dato.



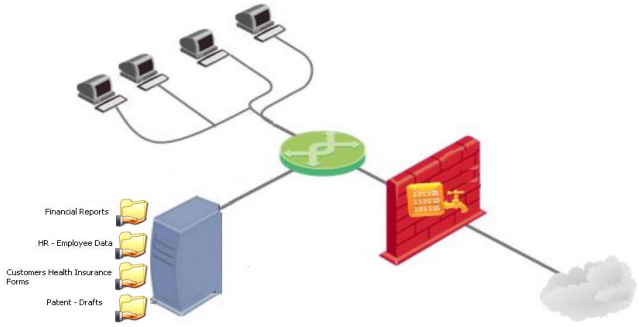
9.7 DATA LOSS PREVENTION (DLP)

El *Software Blade* de Prevención de pérdida de datos (DLP) de Check Point protege de las fugas involuntarias de información sensible, educando a los usuarios sobre políticas adecuadas de manejo de datos y capacitándolos para remediar incidentes en tiempo real.

Esta solución implementada en la red en modo *inline*, se ejecuta en cualquier *Gateway* de Check Point existente, para datos transmitidos en los protocolos de transporte del tráfico (SMTP, HTTP, HTTPS, TLS, FTP).

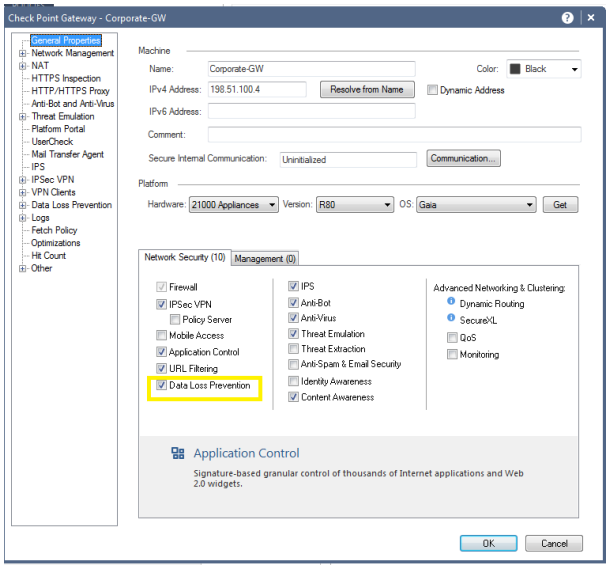
La clasificación de datos MultiSpect™ combina información de usuario, contenido y proceso para tomar decisiones precisas, mientras que la tecnología UserCheck™ permite a los usuarios solucionar incidentes en tiempo real. La solución de DLP auto-educativa basada en la red de Check Point educa a los usuarios sobre las políticas de manejo de datos adecuados.

Las políticas de DLP se crean para definir qué prevenir y cómo prevenir, por política, por segmento de red, por puerta de enlace y/o por grupo de usuarios

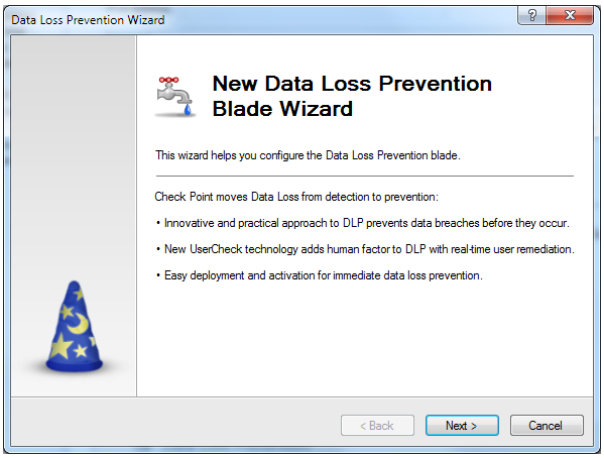


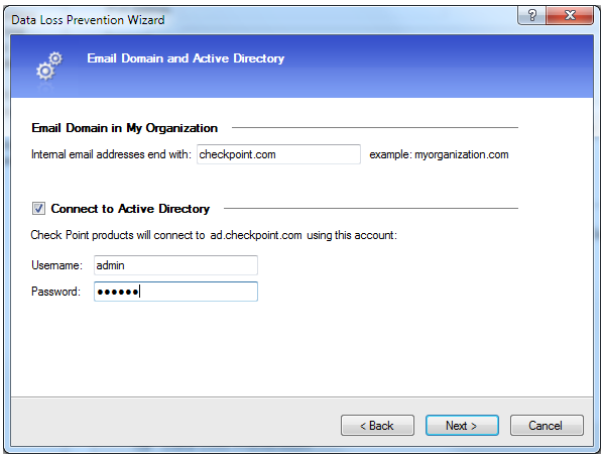
Para configurar DLP:

- Lo primero es habilitar el *Software Blade* de *Data Loss Prevention* en el *Security Gateway/Quantum Spark* correspondiente:

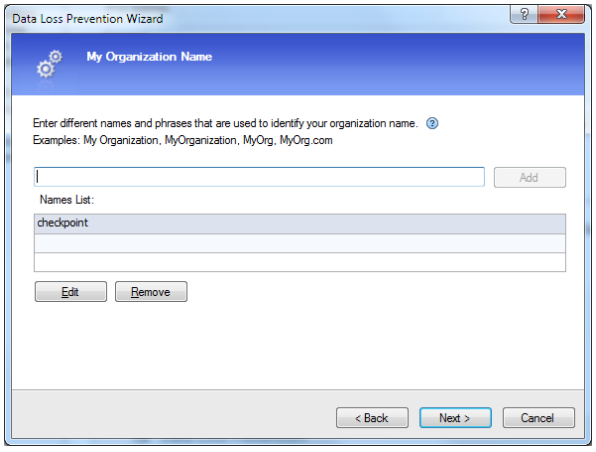


– Seguir el *wizard* de configuración Inicial:

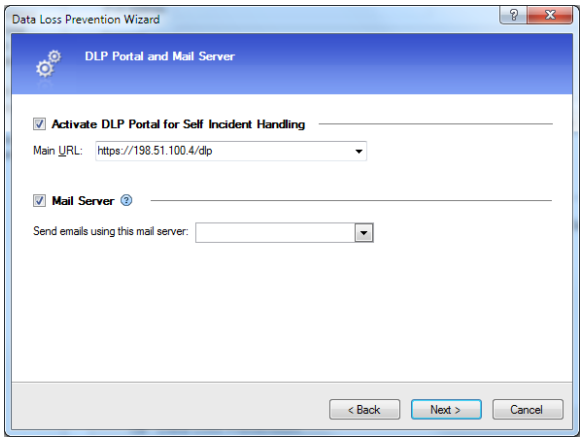




– Establecer el dominio del correo electrónico en la organización para permitir que el *Security Gateway/Quantum Spark* distinga entre las direcciones de correo electrónico internas y externas. Además existe la posibilidad de conectar con *Active Directory* para rellenar automáticamente los usuarios y grupos de usuarios que conforman la definición de la organización.

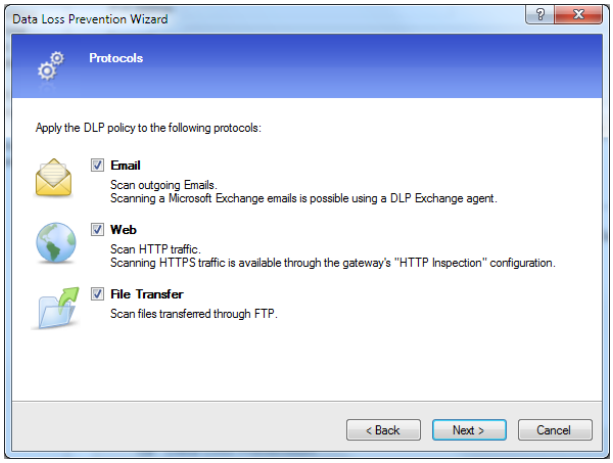


– Introducir diferentes nombres y frases para identificar a la organización. La función DLP usa estos nombres para detectar con precisión los incidentes de pérdida de datos.

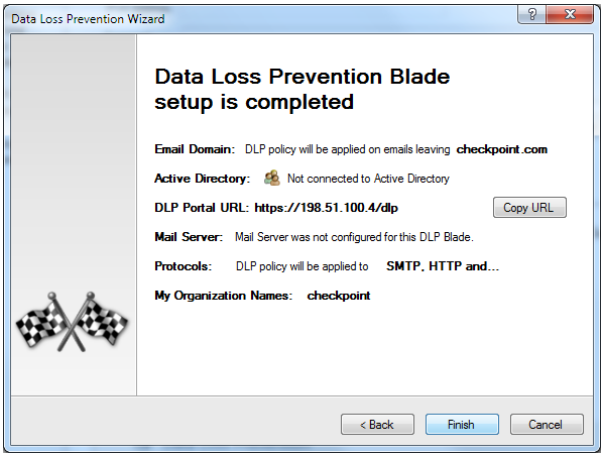


– Activar el portal DLP para el manejo de auto incidentes: seleccione para activar el puerto. La URL predeterminada es *https: // <Gateway IP> / dlp*.

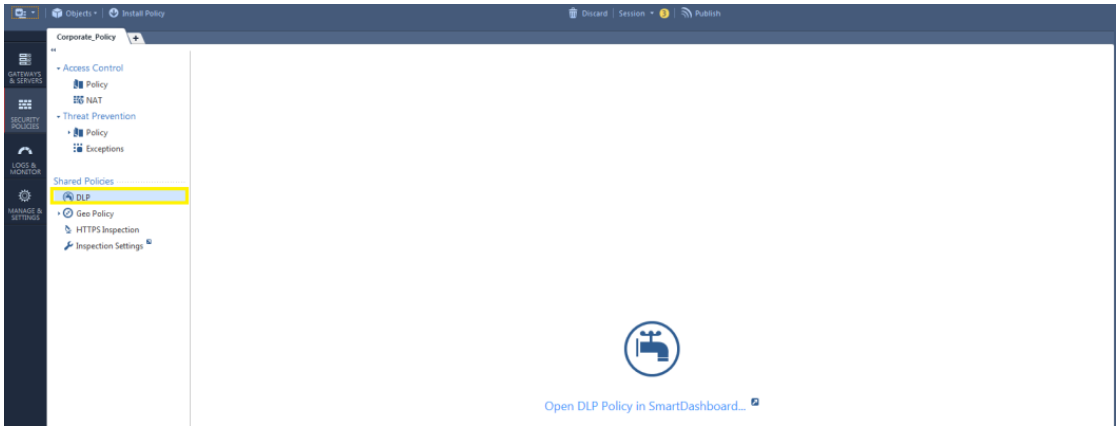
– Además, seleccionar un servidor de correo de la lista de objetos de red existentes o pulse en “Nuevo” y defina un nuevo servidor de correo (SMTP).

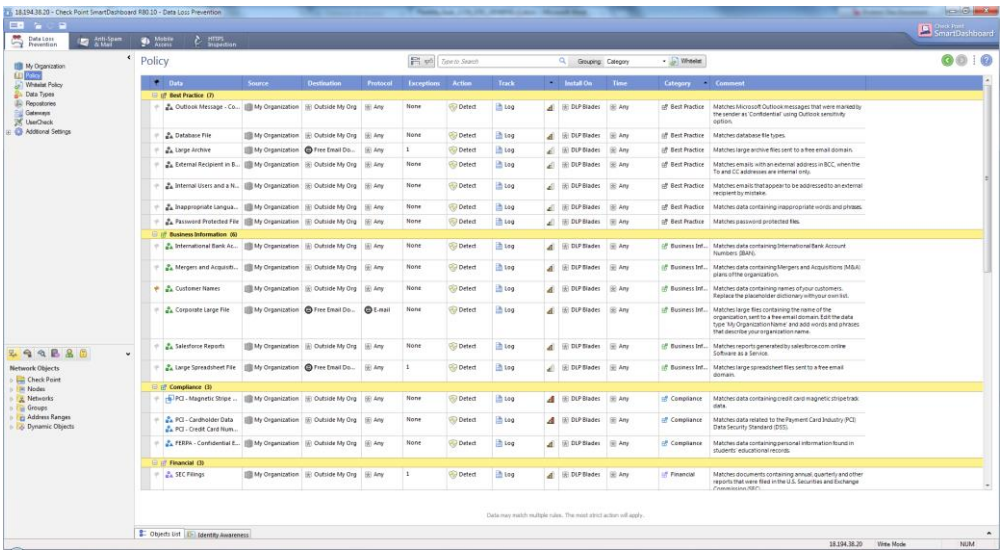


– Seleccionar los protocolos a los que se aplica la política de DLP (SMTP, HTTP, HTTPS y FTP).



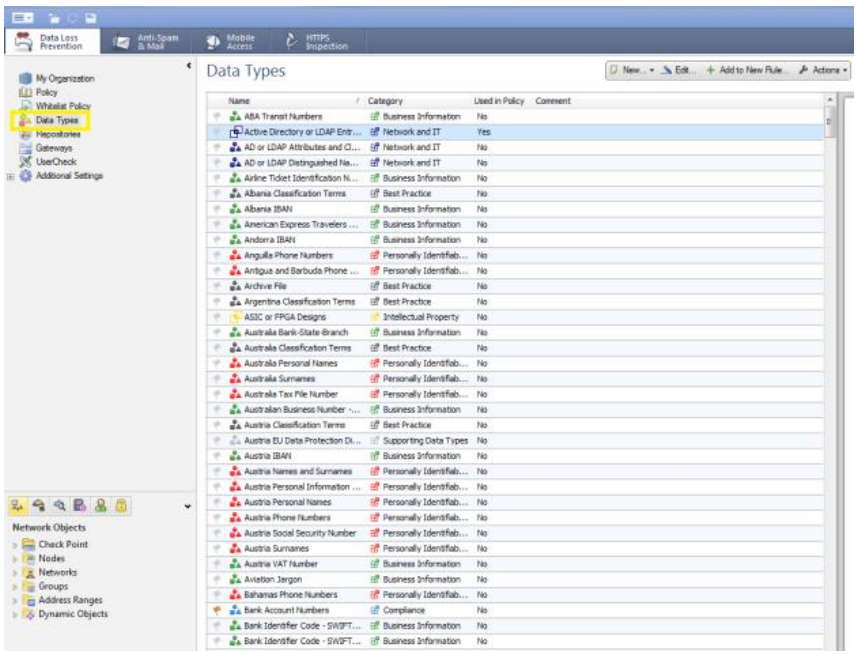
– Acceder al menú de DLP para crear nuevas reglas de seguridad:



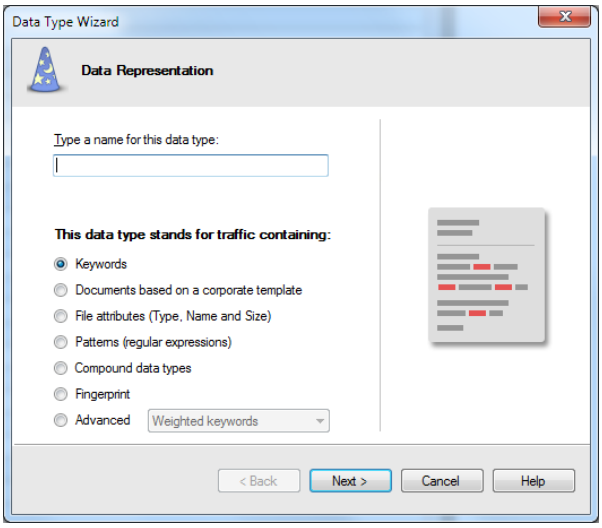


Por defecto vienen creadas una serie de reglas de seguridad para proteger los datos de la organización relacionadas por ejemplo con la perdida de datos personales o números de tarjetas de créditos. Dichas políticas se pueden modificar, eliminar o deshabilitar para crear un conjunto de reglas de seguridad aplicado a la organización.

- Cuando se crea una nueva regla de seguridad, lo primero que hay que definir es el tipo de dato a proteger. Los tipos de datos predefinidos se pueden consultar en: “Data Types”.



- También se pueden crear nuevos tipos de datos:

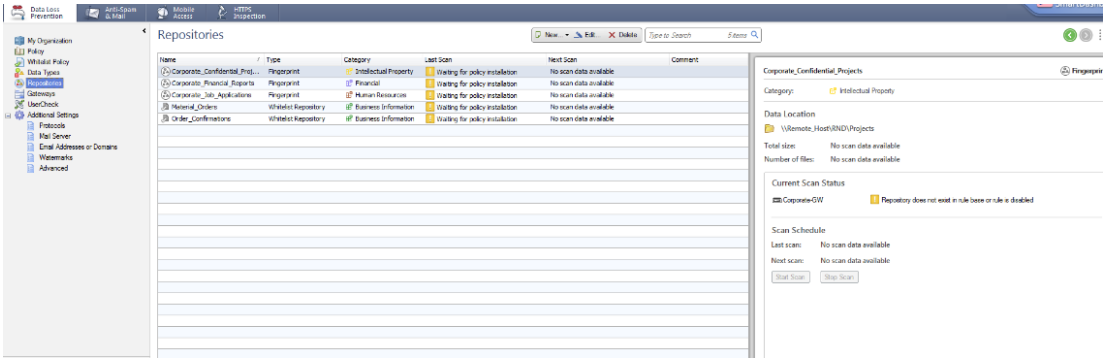


Se pueden utilizar multitud de opciones para crear nuevos tipos de datos: palabras clave, *templates* de documentos, atributos de ficheros, *patterns* o expresiones regulares, tipos de datos compuestos (combinando distintos tipos), *fingerprints*, etc.

Una vez fijado el tipo de datos a machear después se decide el origen y el destino de dicho tráfico (Toda la organización, un grupo de AD determinado, fuera de mi organización,…).

Por último es necesario fijar el protocolo, la acción (Detectar, prevenir, o mostrar mensaje al usuario: *usercheck*) y el seguimiento (log, email, snmp trap,…).

También es posible escanear repositorios para detectar fugas de datos:



9.8 CONTENT AWARENESS

La funcionalidad de *Content Awareness* se usa para controlar los tipos de datos que los usuarios pueden transmitr como por ejemplo:

- PCI: números de tarjeta de crédito.
- HIPPA: Número de registros médicos – MRN.
- Archivo de *visorPDF*.
- Archivo ejecutable.

Además, proporciona visibilidad y control sobre las transferencias de datos en el tráfico de red, inspecciona los flujos de contenido y aplica políticas en los protocolos TCP más utilizados. Una política efectiva requiere:

- Seleccionar tipos de datos y grupos de usuarios.
- Seleccionar diferentes palabras clave o patrones.
- Registros de supervisión y correlación de eventos.

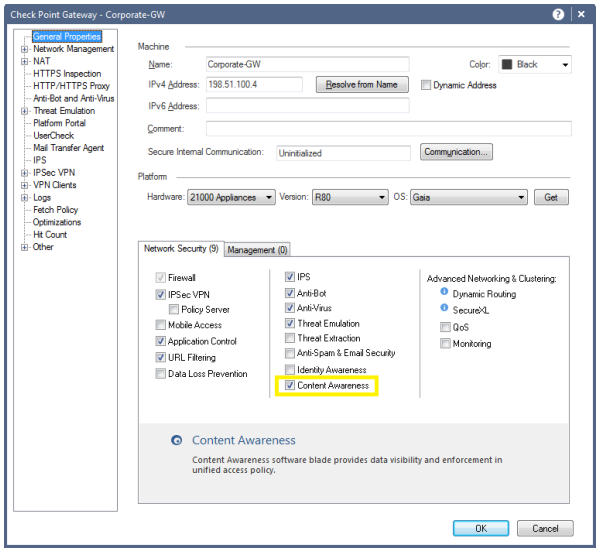
Una regla de política de *Content Awareness* puede configurarse para:

- Permitir que los archivos se descarguen pero no que se suban a Dropbox.
- Permitir que subir imágenes pero no documentos a Facebook.
- Permitir solo el envío de la tarjeta de crédito a través de HTTPS (y no HTTP).

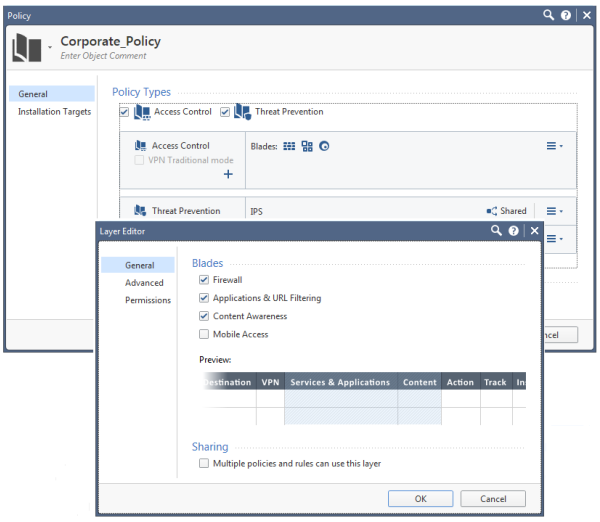
Aunque parezca que se trata de funcionalidades muy similares, *Content Awareness* y DLP son *Software Blades* separados, que coexisten de forma independiente. En el caso de DLP tiene una Base de reglas dedicada, admite tipos de datos avanzados, como *fingerprints*. También soporta poner correo electrónico en cuarentena cuando se ha detectado una fuga de datos.

Por otro lado, *Content Awareness* es parte de la Base de reglas unificada, se puede usar como una capa dedicada. Esta soportado para despliegues en VSX o IPV6. Escanea el tráfico entrante y saliente y se puede configurar con granularidad en cada regla. Para su configuración:

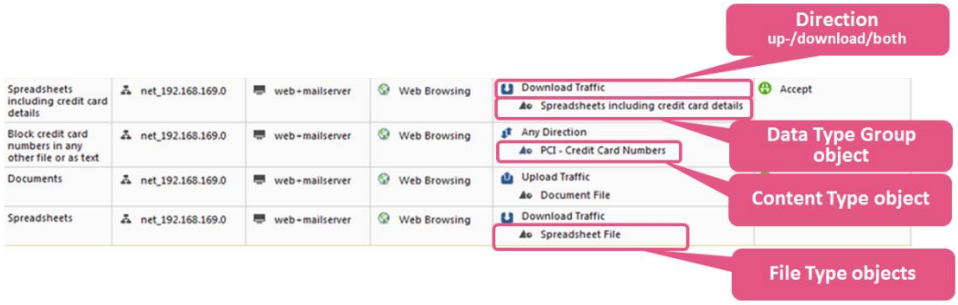
- Lo primero es habilitar el Software Blade de Content Awareness en el Security Gateway/Quantum Spark correspondiente:



– El siguiente paso es habilitar el Software Blade de Content Awareness en la capa de la política de seguridad oportuna:



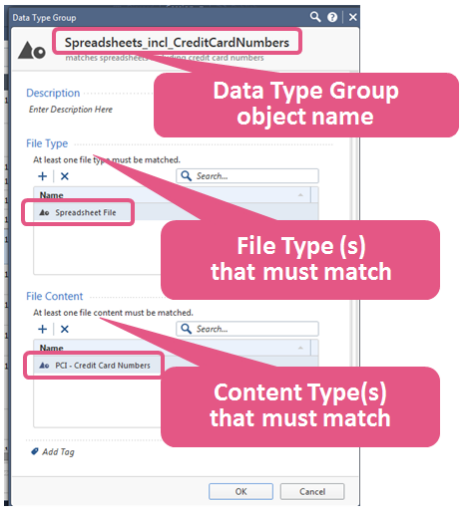
– Crear una regla de seguridad. Aparecerá una nueva columna denominada “Content”:



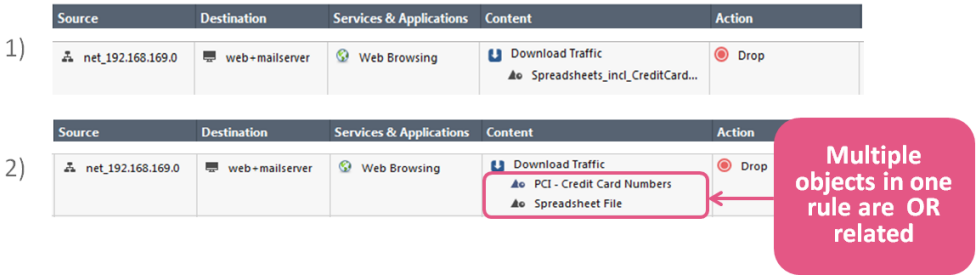
– Dentro de la columna data tenemos varios settings que configurar:

- Tipo de dato.
- Tipo de fichero.
- Combinación de varios tipos de datos o tipos de ficheros.
- Dirección del tráfico (subida, descarga o ambas).

– Crear un tipo de datos combinado *New* ➔ *Data Type* ➔ *Data Type Group*.



Nota: Si se añaden tipos de datos y tipos de ficheros en la columna "Content" es como si se aplicase el operador lógico "OR" si crea un tipo de datos combinado es como si se aplicase el operador lógico "AND".



10. PLANO DE PREVENCIÓN DE AMENAZAS

En este apartado se tratarán las funcionalidades existentes en el plano de prevención de amenazas. Entre ellas, funcionalidades específicas de seguridad para controlar las vulnerabilidades, la descarga de malware, el acceso a sitios webs maliciosos o de *phishing*, etc.

10.1 IPS

El *Software Blade* de IPS de Check Point aprovecha la capacidad de rendimiento de los procesadores multi-núcleo. La *suite* de tecnologías de Check Point trata de cubrir las necesidades en un despliegue de IPS en-línea:

– Seguridad: La primera tarea de un IPS es bloquear ataques. Algunos ataques emplean herramientas y técnicas conocidas, otros desconocidas. El IPS debería ser capaz de prevenir ataques de Día Cero y evitar falsos positivos. Para conseguirlo se deben emplear métodos de detección para amenazas conocidas y desconocidas: tener disponible una base de datos con firmas que te protejan contra vulnerabilidades conocidas, detección de código malicioso, comportamientos anómalos, anomalías de protocolo, detectar inyección de código mediante HTML, SQL y LDAP, o intentos de *Phissing*.

- Alto rendimiento: La solución IPS debe ser rápida, sin importar que hayas activado las funciones de análisis más intensas.
- Preciso: Para minimizar falsos positivos ya que estos puede causar que se pase por alto problemas reales de seguridad al encontrarse un volumen excesivo de eventos irrelevantes o sin importancia.
- Fiable: Cumplir los SLA. La solución debe ser lo suficientemente predecible para probar el sistema en modo pasivo, y ajustarlo para prevenir que la conectividad se mantiene bajo cualquier escenario.
- Actualizable: Recibir continuamente las firmas más recientes. Debe tener la capacidad de evolucionar para identificar los tipos de ataque más cambiantes. Una práctica común entre los creadores de malware es probar sus ataques contra antivirus populares y modificar la firma del ataque ligeramente para prevenir que sea detectado. Una solución IPS debe ser capaz de actualizarse casi en tiempo real para permitir a los administradores parchear los sistemas vulnerables.
- Control granular: Habilidad para aplicar sólo las restricciones que son necesarias, con herramientas forenses integradas para análisis *post-mortem*.
- Geo protecciones: Fuerza o vigila el tráfico en función del origen o del país de destino. Crea una política de geo-protección con excepciones para permitir el tráfico legítimo mientras que bloquea o controla el tráfico de fuentes desconocidas y de las que no se confía. Se supervisa la actividad con el *SmartEvent Software Blade*.

En resumen, el IPS proporciona una protección completa para vulnerabilidades de servidores, clientes, sistemas operativos, red y otros. El motor de detección de amenazas multicapa combina firmas, validación de protocolo, detección de anomalías, análisis de comportamiento y otros métodos para proporcionar protección en la red.

Combinado con la protección multicapa de diferentes *Software Blades* de Check Point, el IPS puede aplicarse además solo a las partes de tráfico necesarias, con diferentes perfiles de protección granularizables.

Check Point proporciona un motor de búsqueda de patrones para identificar ataques conocidos en contextos específicos de la secuencia de paquetes.

- Passive Streaming Library: La tecnología de *Passive Streaming Library* (PSL) detecta paquetes que pueden llegar desordenados o pueden ser retransmisiones legítimas de paquetes que aún no han recibido un acuse de recibo. La capa PSL proporciona a las aplicaciones una secuencia coherente de datos que está libre de varios problemas de red o ataques.
- Protocol Parsers: Los analizadores de protocolo ensamblan los datos para una inspección adicional mediante otros componentes. Además, realizan varias comprobaciones de seguridad como la validación de conformidad de protocolos con las RFC y comprobación de anomalías de protocolo.
- Context Management Infraestructure (CMI): Coordina diferentes componentes, decide qué protecciones se deben ejecutar en un cierto paquete, decide la acción final que se realizará en el paquete y emite un registro de eventos, incluida una referencia CVE si corresponde.

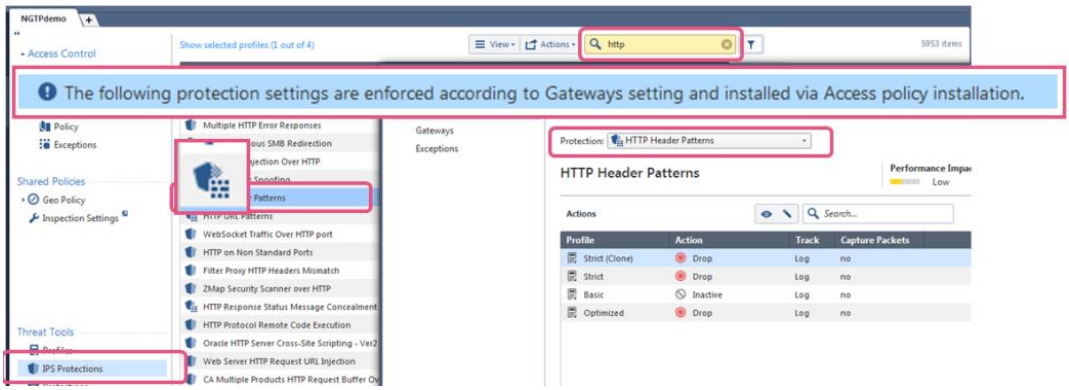
- Pattern Matcher: Es un motor clave dentro de la arquitectura de aplicación, identificando rápidamente paquetes inofensivos, firmas comunes en paquetes maliciosos, y aporta un segundo nivel de análisis para reducir falsos positivos.
- Compound Signature Identification (CSI): Hace sofisticadas inspecciones de firmas e identificación de aplicaciones. Puede reconocer firmas de múltiples partes del tráfico con el fin de identificar una actividad maliciosa. CSI puede aplicar firmas en múltiples partes de un paquete, múltiples partes de los protocolos como la URL o la cabecera HTTP, múltiples partes de la conexión, como una solicitud y respuesta CIFS, o múltiples conexiones, como control de voz IP o conexiones de datos.
- INSPECT: Se usa para detectar ataques complejos y evasivos.
- Geo-Protección: Monitorización o bloqueo del tráfico en base al país origen o destino.

Además es importante entender las tres características que se utilizan para clasificar las distintas protecciones (no sólo las protecciones de IPS):

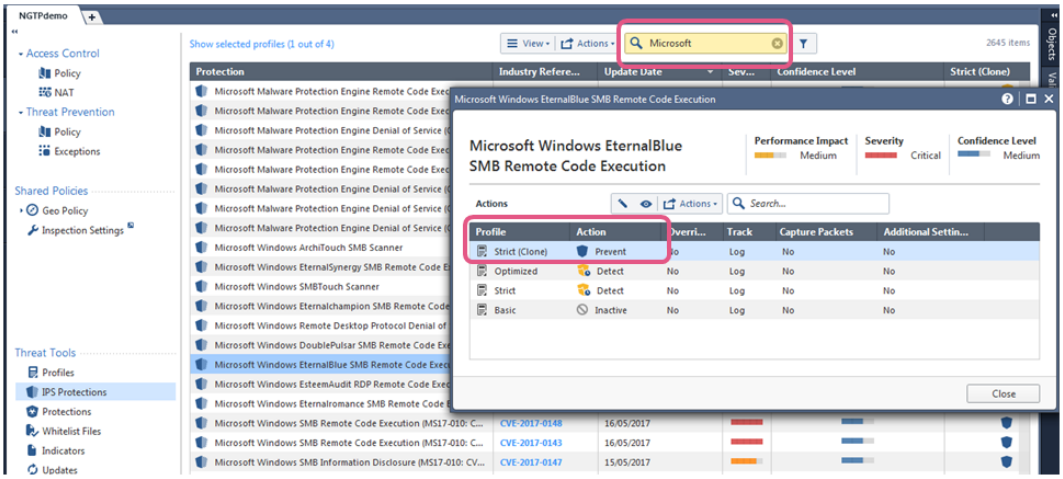
- Gravedad: Debe activar las protecciones de Gravedad al menos Crítica y Alta, a menos que esté seguro de que no desea activar la protección especificada.
- Por ejemplo, si una protección tiene una clasificación de Severidad Alta e Impacto de rendimiento Crítico, asegúrese de que la protección sea necesaria para su entorno antes de activar la protección.
- Nivel de confianza: Algunos tipos de ataques son menos severos que otros, y el tráfico legítimo a veces puede ser reconocido erróneamente como una amenaza. El valor de nivel de confianza muestra qué tan bien la protección especificada puede reconocer correctamente el ataque especificado. Nivel de falsos positivos.
- Impacto en el rendimiento: Algunas protecciones requieren el uso de más recursos o se aplican a tipos comunes de tráfico, lo que afecta negativamente al rendimiento de los *Security Gateways* en los que se activan.

Además, las protecciones IPS se dividen en dos tipos principales:

- *Core Protections:* Estas protecciones se incluyen en el producto y dependen de las opciones de configuración. Son parte de la política de control de acceso y son administradas en un perfil dedicado con una asignación dedicada a los *Security Gateways*.

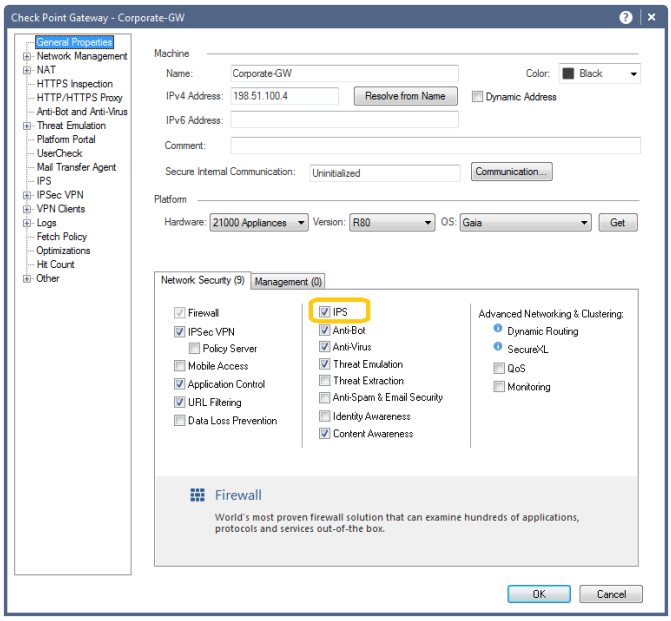


– ThreatCloud Protections: Protecciones actualizadas desde la nube de Check Point. Estas protecciones son parte de la política de prevención de amenazas. En este caso se administran mediante el propio perfil de *Threat Prevention*.

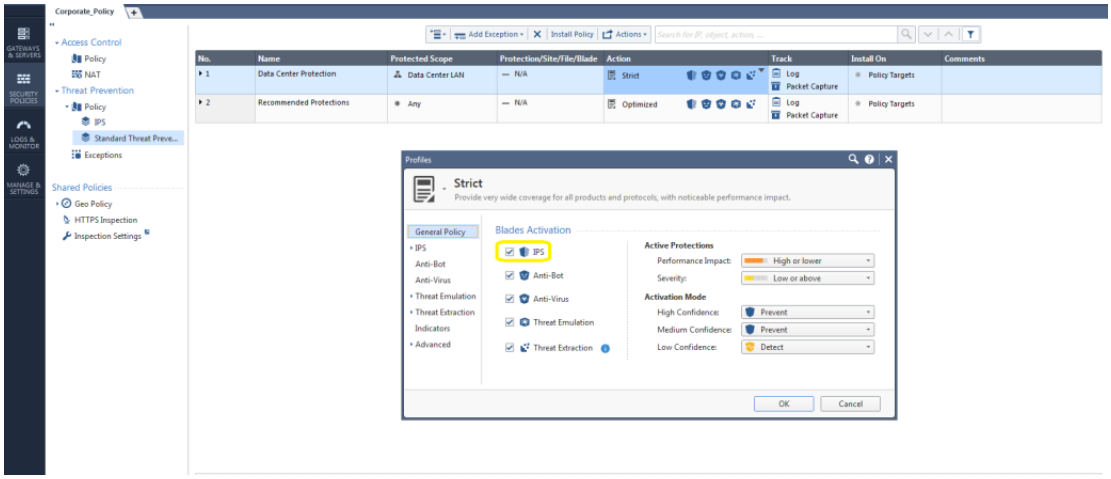


Para su configuración:

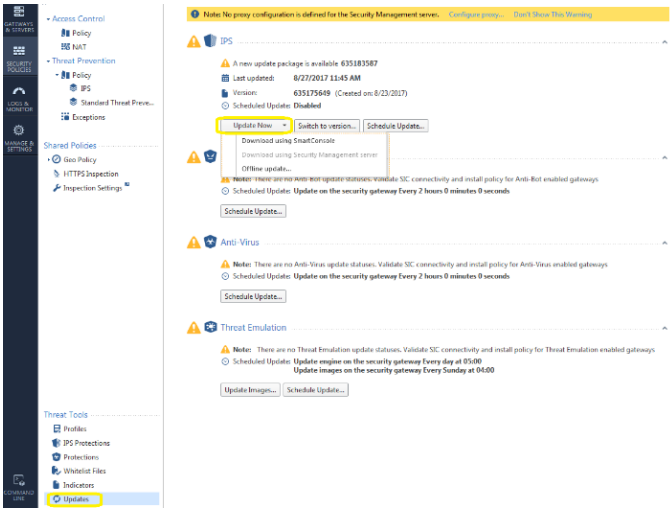
– Lo primero es habilitar el *Software Blade* de "Application Control" en el *Security Gateway/Quantum Spark* correspondiente:



– El siguiente paso es habilitar el *Software Blade* en el perfil de las políticas de *Threat Prevention*:



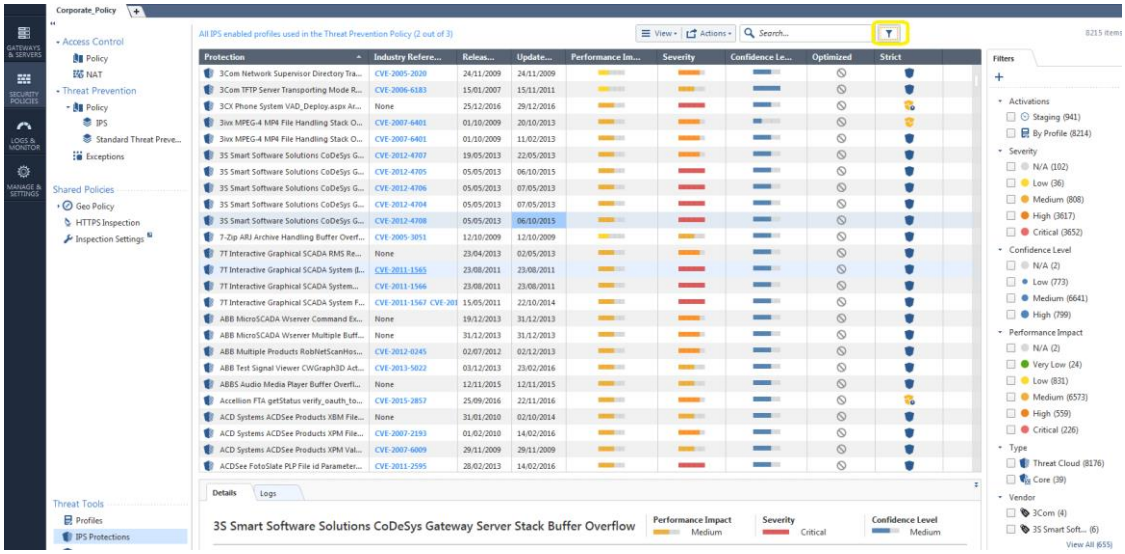
– Es importante actualizar las firmas, para ello navegar a las *Threat Tools* ➔ *Updates.*



Se pueden actualizar las firmas usando el *SmartConsole*, usando la propia consola de gestión o haciendo una actualización offline.

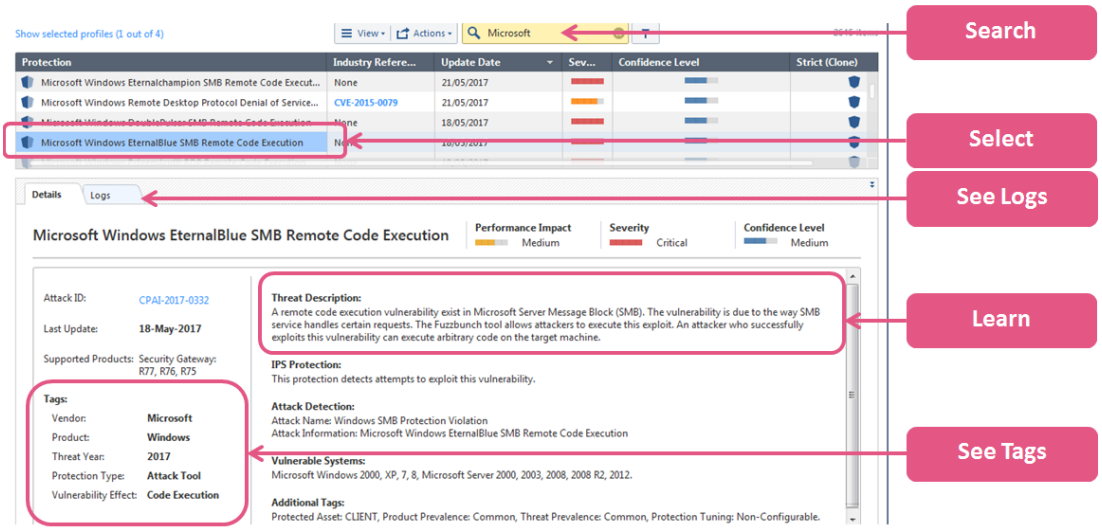
Lo mejor es programar la actualización de las firmas todos los días a una determinada hora mediante *Schedule Update*.

Navegar a las protecciones IPS *Threat Tools* ➔ *IPS Protections.*



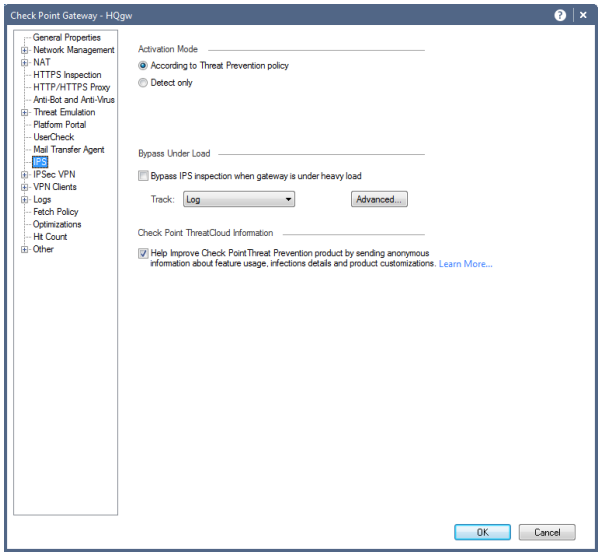
Puede buscar las protecciones por nombre de protección, motor o por cualquier tipo de información que se muestra en las columnas y ver cuál es su estado en cada uno de los perfiles de *Threat Prevention*.

Si entramos en detalle en las propias protecciones, cuando pinchamos en una de ellas tenemos la siguiente información al respecto:

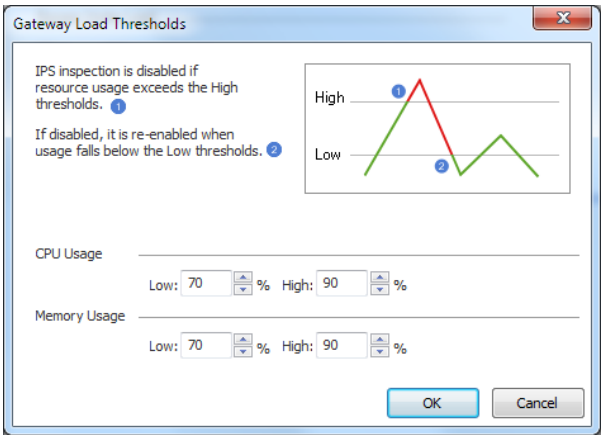


Se puede ver los *logs* relacionados con la propia protección, la descripción de la misma, los *tags* asociados, el CVE, categorización en cuanto a las tres características principales (Impacto en el rendimiento, gravedad y nivel de confianza), la última fecha de actualización, etc.

Configurar que en caso de que el *Security Gateway/Quantum Spark* se encuentre con alta carga deje pasar el tráfico sin inspeccionar. Editar el objeto *Gateway*, navegar a la pestaña de IPS y a la sección “Bypass Under Load”.

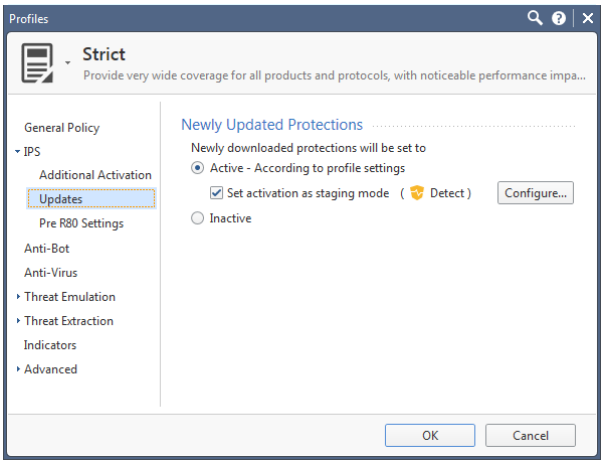


También se pueden fijar umbrales del uso de la CPU como de memoria para lo que se considera que el Security Gateway/Quantum Spark está bajo alta carga de tráfico.

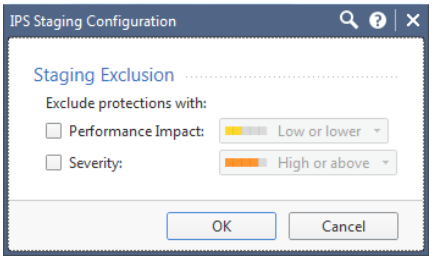


Después de configurar la instalación IPS inicial, la mayoría de las protecciones se implementan en el modo "Prevenir" para que sean bloqueadas, aunque algunas permanecen en modo "Detectar" para un análisis adicional.

Continuamente surgen nuevas amenazas y el tráfico de la red cambia con nuevas aplicaciones, servicios y protocolos. Las protecciones recién descargadas estarán en modo de prueba (*Staging Mode*). Editar el perfil de *Threat Prevention* y navegar a la sección *IPS* ➔ *Updates.*

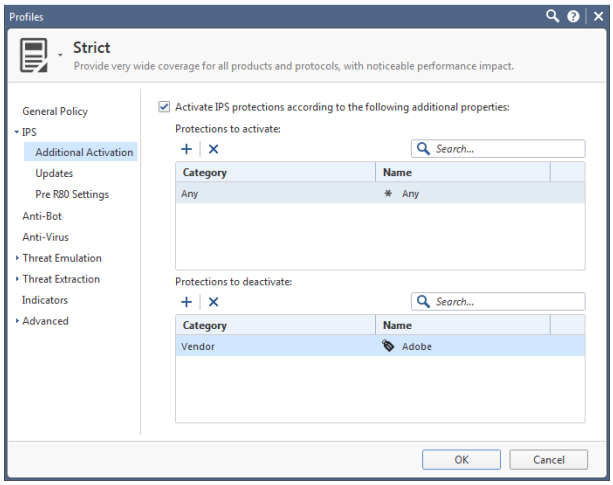


Además se pueden configurar exclusiones al *Staging Mode* pinchando en el botón de configurar, teniendo en cuenta el impacto en el rendimiento o la criticidad.



Más adelante hay que revisar los eventos de estas protecciones y cambiar su modo de Staging a Detect para luego ejecutar un análisis de las nuevas protecciones y determinar si finalmente pueden ejecutarse en modo “Prevenir”.

Por último, existe la posibilidad de añadir o excluir protecciones directamente por su clasificación mediante las tags que se les asignan. Por ejemplo, se pueden eliminar las protecciones de un determinado “vendor”.



10.2 ANTIVIRUS

El Software Blade Check Anti-Virus usa en tiempo real las firmas de virus y protecciones basadas en anomalías de *ThreatCloud™*, para detectar y bloquear el malware en el *Gateway*

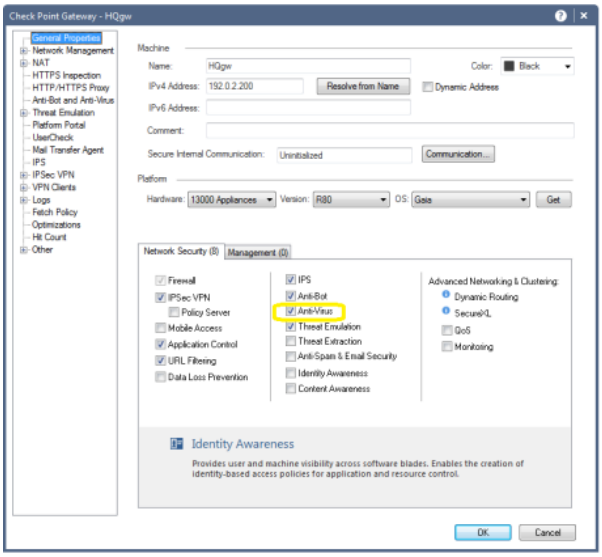
antes de que los usuarios se vean afectados. De esta forma, se proporciona al *Gateway* inteligencia en tiempo real.

El Anti-Virus protege contra amenazas transmitidas a través de los protocolos HTTP, HTTPS, FTP y SMTP e IMAP. Hace uso de diferentes motores y protecciones:

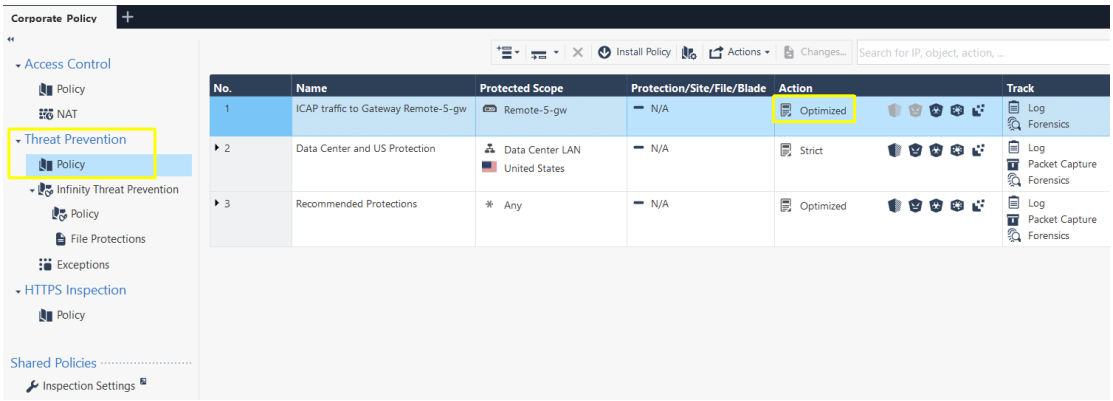
- Motor de reputación: Para analizar enlaces dentro de correo electrónico y URL que pueden contener malware.
- Motor de firmas: Con firmas de virus reconocidos.
- Motor de patrones de comportamiento.
- Protecciones ante actividad inusual.
- Motor de tipos de fichero. Con 89 tipos de fichero reconocidos, en base a los que se puede granularizar la política para inspeccionar, permitir o bloquear.

Para su configuración:

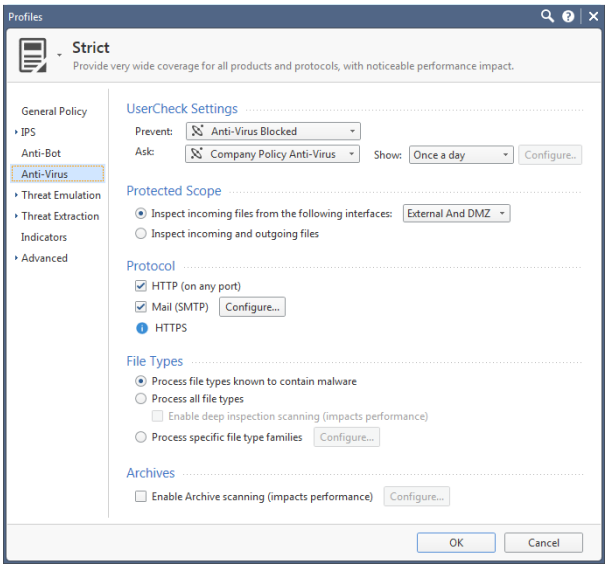
- Lo primero es habilitar el Software Blade de "Antivirus" en el Security Gateway/Quantum Spark correspondiente:



- El siguiente paso es habilitar el Software Blade en el perfil de las políticas de Threat Prevention.



- Navegar a la sección de Anti-Virus:



El primer apartado es el de *UserCheck* para poder definir qué mensajes mostrar al usuario en caso de que se detecte un evento de *Antivirus*.

- Prevent: Seleccionar el mensaje UserCheck que se abrirá ante un evento cuya acción sea prevenir.
- Ask: Seleccionar el mensaje UserCheck que se abrirá ante un evento cuya acción sea preguntar. Y con qué frecuencia se mostrará el mensaje.

En la sección "Protected Scope" se definirá tanto el tipo de interfaz como la dirección del tráfico que será protegido.

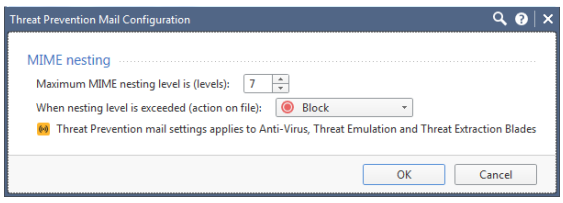
Inspeccionará ficheros entrantes desde las siguientes interfaces:

- Interfaz externa.
- Interfaz externa y DMZ.
- Todas las interfaces.
- Inspeccionará todos los ficheros entrantes y salientes.

En cuanto a los protocolos sobre los que se aplicará la funcionalidad de Anti-Virus tenemos distintas opciones:

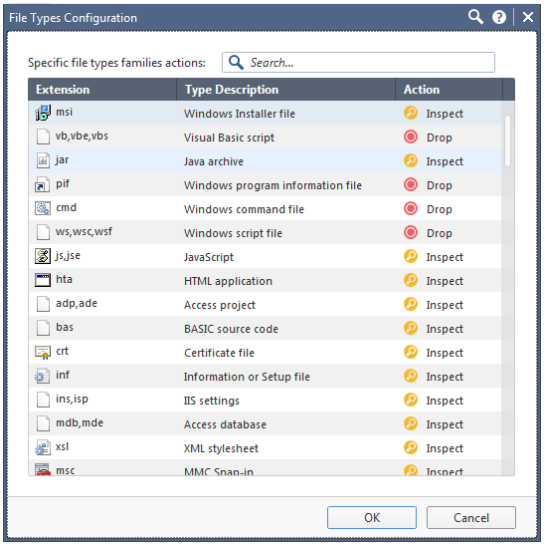
- HTTP (en cualquier puerto).
- Mail (SMTP).
- HTTPS en caso de que se habilite HTTPS Inspection.

En caso de proteger SMTP hay varias opciones de configuración:



Configuración de anidamiento MIME establece el número máximo de niveles en cuanto al anidamiento MIME que el motor *ThreatSpect* escanea en el correo electrónico. Cuando se excede el nivel de anidamiento se configura si la acción será bloquear o permitir el archivo.

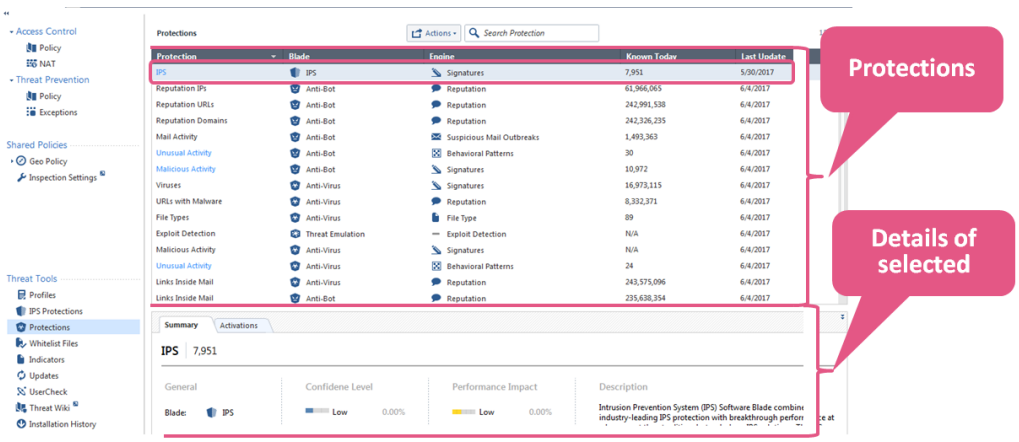
También se puede seleccionar el tipo de archivos:



Para cada de tipos de archivo, seleccione la acción *Antivirus* que se llevará acabo (*Inpsect*, *Drop*, *Bypass* o *Deepscan*).

Para habilitar el escaneo de archivos establezca la cantidad en segundos para detener el procesamiento del archivo. El valor predeterminado es 30 segundos. Configurar para bloquear o permitir el archivo cuando se excede el tiempo máximo.

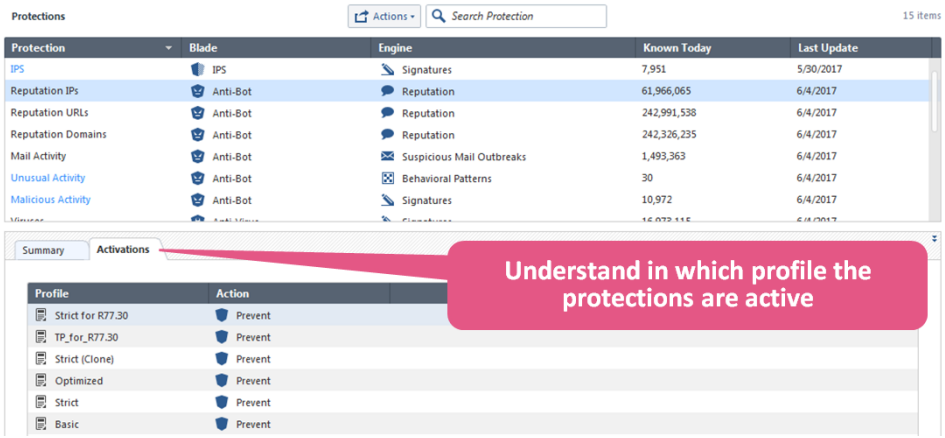
Navegar por las protecciones de los *blades* de *Anti-Virus* y *Anti-Bot*:



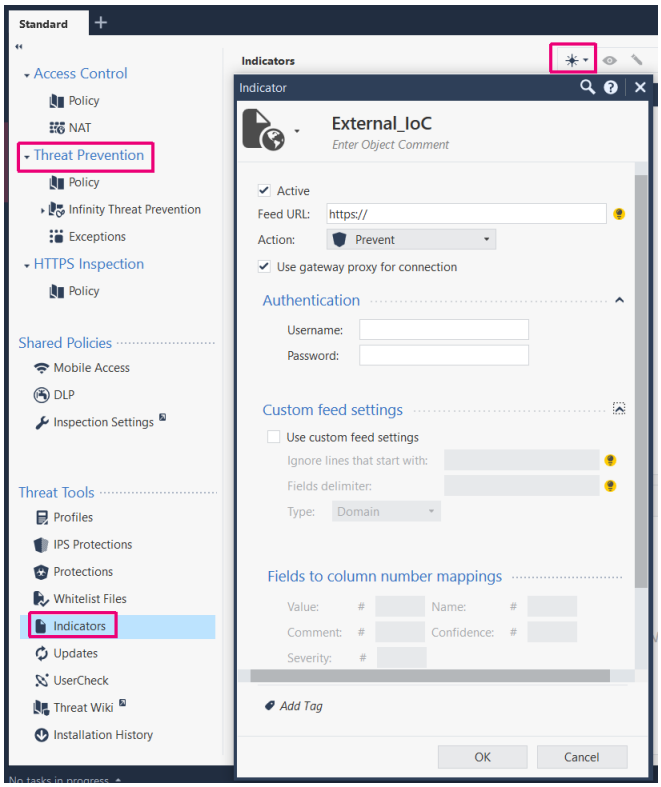
Cada tipo de protección se clasifica por el *blade* que lo detecta y previene y por el tipo de motor de detección (firmas, reputación, patrones de comportamiento, etc).

Además cada protección viene detallada por su nivel de criticidad, nivel de confianza e impacto en el rendimiento del equipo:

Si queremos ver en qué perfil esta activa dicha protección sólo tenemos que pinchar en la pestaña de "*Activations*".



Importar indicadores de compromiso, en el menú de las "Threat Tools", seleccionar "*Indicators*". También existe la opción de añadir una URL externa desde la que se descarguen y mantengan actualizados indicadores de comprimiso. Para esto, se puede utilizar la opción de añadir un "External IoC File".



10.3 ANTIBOT

El *Software Blade* de *Anti-Bot* detecta máquinas infectadas por bots bloqueando las comunicaciones de Command and Control (C&C). Se actualiza en *ThreatCloud™*.

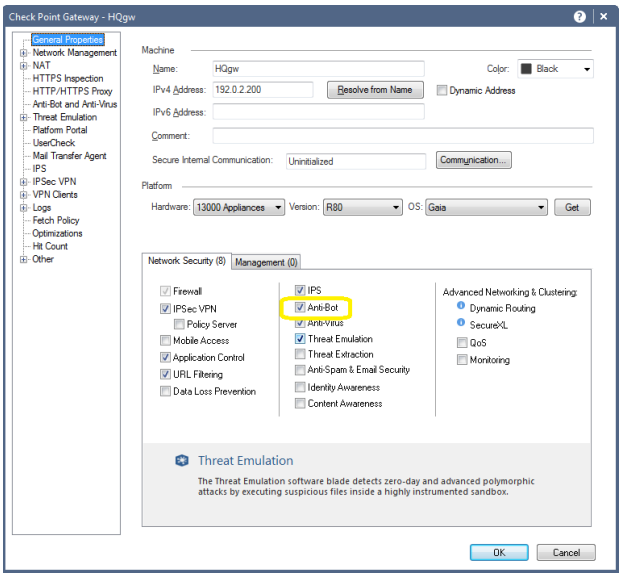
Un Bot es un software malicioso que invade el ordenador, normalmente de forma silenciosa. Los bots permiten a los delincuentes controlar de forma remota el equipo para ejecutar actividades ilegales como robo de datos, spam, difusión de software malicioso y participar en ataques de DOS sin su conocimiento. Los Bots juegan un papel clave en los ataques dirigidos, amenazas persistentes avanzadas (APT).

El Anti-Bot *Software Blade* de Check Point (inspección multi-capa *ThreatSpect™*) detecta infecciones mediante la correlación de múltiples métodos de detección:

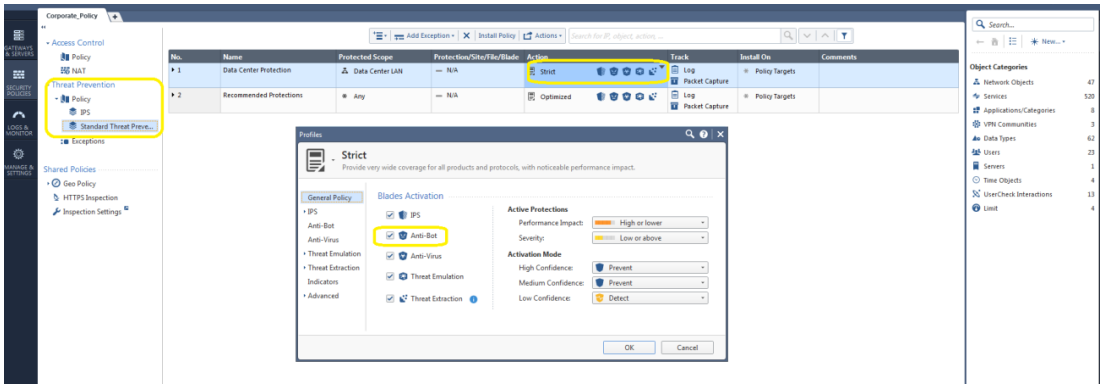
- Motor de reputación: Con enlaces a analizar en correo electrónico, dominios y URL utilizadas por *bots* así como direcciones IP maliciosas.
- Motor de firmas: Con firmas de detección de actividad maliciosa de *bots*.
- Motor de patrones de comportamiento: Con detección de actividad inusual relacionada con *bots*.

Para su configuración:

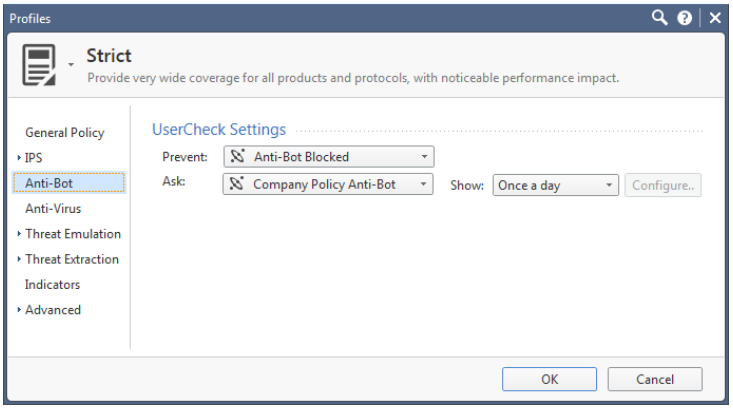
- Lo primero es habilitar el Software Blade de “Anti-Bot” en el Security Gateway:



- El siguiente paso es habilitar el Software Blade en el perfil de las políticas de Threat Prevention:



– Navegar a la sección de Anti-Bot:

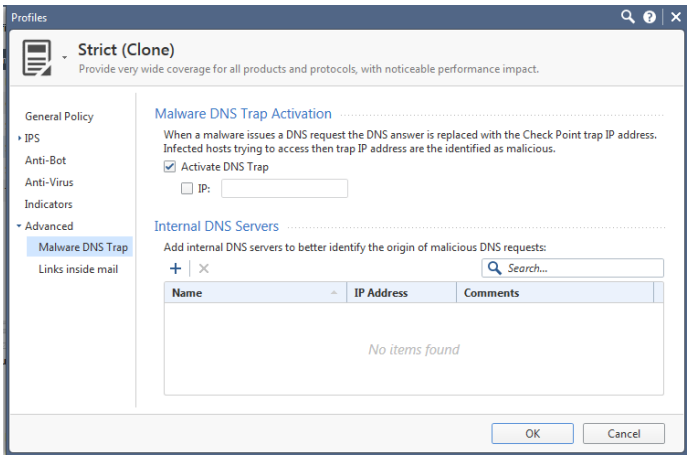


El apartado de *UserCheck* sirve para poder definir qué mensajes mostrar al usuario en caso de que se detecte un evento de *Anti-Bot*.

– Prevent: Seleccionar el mensaje *UserCheck* que se abrirá ante un evento cuya acción sea prevenir.

– Ask: Seleccionar el mensaje *UserCheck* que se abrirá ante un evento cuya acción sea *Ask*. Y con qué frecuencia se mostrará el mensaje.

También existe la opción de configurar DNS *Traps*, para responder a una consulta DNS para una *botnet* conocida con una dirección IP falsa. De esta forma el *host* que intente acceder a esa IP es clasificado como infectado. Dentro del perfil de *Threat Prevention*, seleccionar "Advanced" y después "*Malware DNS Trap*":



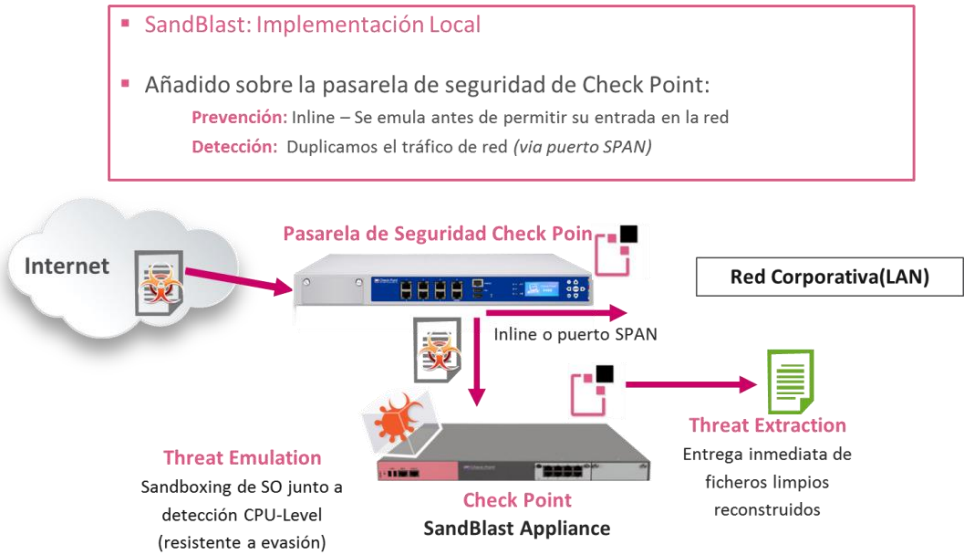
10.4 SANDBLAST NETWORK

La implementación de esta tecnología de mitigación y prevención de amenazas avanzadas está basada en dos componentes principales, *Sandblast Threat Emulation* y *SandBlast Threat Extraction*, ambos componentes son complementarios y aportan una aproximación diferente al problema. Mientras *Threat Emulation* se basa en detección de indicadores o comportamientos maliciosos del malware una vez "detonado", *Threat Extraction* se basa en limpiar preventivamente los documentos (principal vector de infección) y eliminar todo el contenido susceptible de ser utilizado para atacar.

Cuando ambos componentes trabajan coordinados, el resultado final es que el usuario recibe un fichero limpio en tanto se diagnostica la "benignidad" o no del fichero original y se le concede acceso a éste último cuando el diagnóstico es favorable. De esta forma se elimina una de las principales desventajas de los sistemas basados en *SandBoxing*, el retardo en el diagnóstico. Este sistema funciona tanto para correo como para navegación web (vehículos principales de la distribución del malware).

En tanto que *Sandblast Threat Extraction* puede implementarse directamente en línea y toda la funcionalidad se procesa en una pasarela de seguridad, debido a su naturaleza y la carga de procesamiento que genera, no se recomienda que se realice en el mismo *Gateway* que procesa el tráfico y extrae los ficheros objeto de análisis.

Para ello existen dos posibilidades, la primera es hacer el análisis en la nube de Check Point y la segunda es descargar esta funcionalidad en equipos especializados locales (más de uno si queremos proveer de redundancia a esta funcionalidad), que se ocuparán de realizar el sandboxing y diagnóstico de los ficheros.



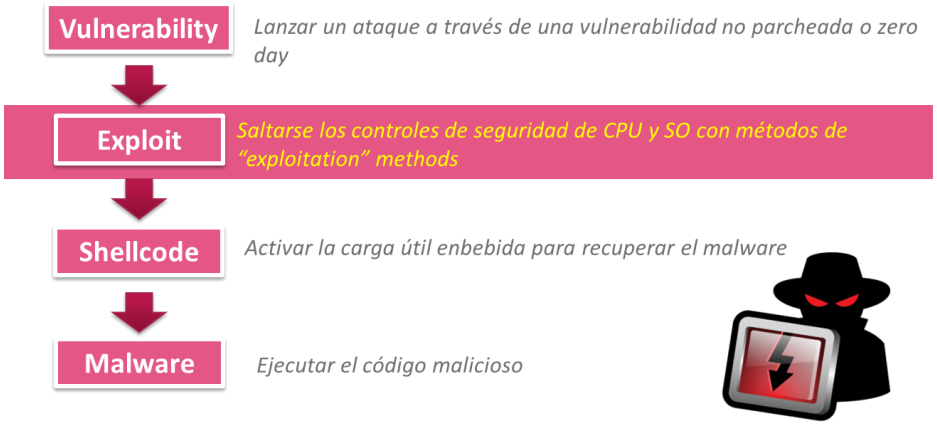
10.4.1 THREAT EMULATION

Una de las capacidades principales de la tecnología *SandBlast* es su resistencia a evasión frente a malware que, de forma inteligente, intenta evitar su detección. Dispone de medidas tradicionales para intentar detectar comportamientos de este tipo (aceleración del reloj,

detección de evasión basada en entorno virtual, detección de comportamiento humano como pulsaciones de teclado…etc), técnicas de *machine learning* y comportamiento, análisis adicional con firmas para detectar sub-variantes y otras técnicas para detectar/provocar los efectos del malware una vez detonado.

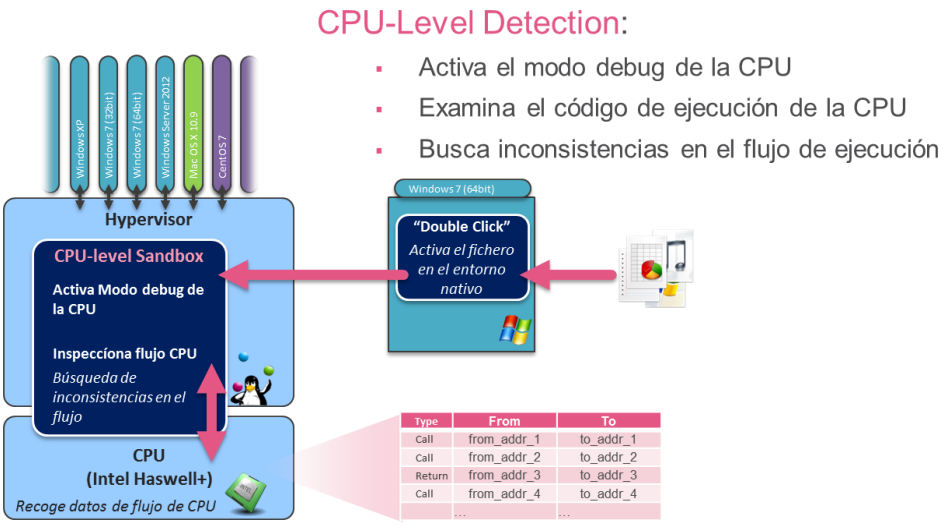
Se ha embebido en el sistema una tecnología que puede detectar comportamientos maliciosos antes incluso de que tengan la oportunidad de establecer medidas de evasión. Esta tecnología es denominada *CPU Level Detection* y su funcionamiento, desde el punto de vista conceptual es bastante simple.

El proceso simplificado de un ataque es el siguiente:



Si nos centrásemos en el *Shellcode* y malware, y sus efectos en ejecución, el problema es que podemos ser víctimas de técnicas novedosas de evasión (y entonces estaríamos un paso por detrás de los creadores de malware por lo que no estaríamos consiguiendo el objetivo de ser preventivos desde el primer momento, no habría demasiada diferencia frente a soluciones basadas en firmas). Ahora bien, esta tecnología lo que hace es centrarse en la detección de las técnicas de evasión de los controles de seguridad de CPU y Sistema Operativo, estos métodos son muy conocidos y no evolucionan más allá de un par de técnicas nuevas o variaciones de las conocidas al año, por lo que la velocidad de evolución permite estar siempre actualizado desde el punto de vista de detección.

Estas técnicas conocidas son, por ejemplo *ROP, Heap Spraying*…etc y están diseñadas como evasiones de los controles de seguridad del SO (no se puede ejecutar una zona de memoria marcada como datos, las direcciones de memoria virtual se hacen aleatorias para evitar predictibilidad…). La tecnología CPU Level Detection se centra en la detección de estas técnicas analizando, mediante la tecnología proporcionada por INTEL en sus procesadores, las trazas de ejecución del sistema, *stack* de ejecución y llamadas, interrupciones, etc.



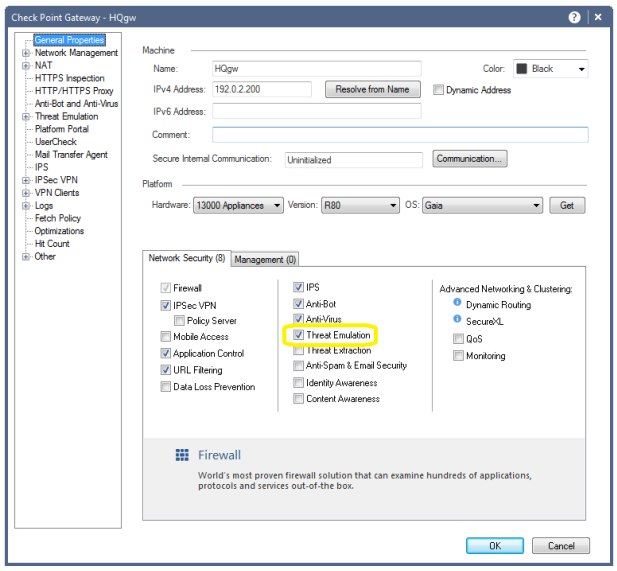
Esta tecnología de *sandboxing* soporta más de 40 tipos de ficheros incluyendo Adobe PDF, Microsoft Office, EXE, ficheros en archivos (cab, zip…), Flash, Java Applets, PIF, análisis de url incrustadas en correos y ficheros…

Una de las ventajas que incorpora la tecnología es la actualización constante y sin necesidad de actualizar la versión ni de la pasarela de seguridad, ni del *appliance* responsable de la emulación en sí, dado que la actualización del motor de detección es suficiente Aademás de la posibilidad de incorporar diferentes entornos de emulación (diferentes versiones de SO como Windows 10, Windows XP…) o incluso versiones personalizadas (plataformadas) por el usuario.

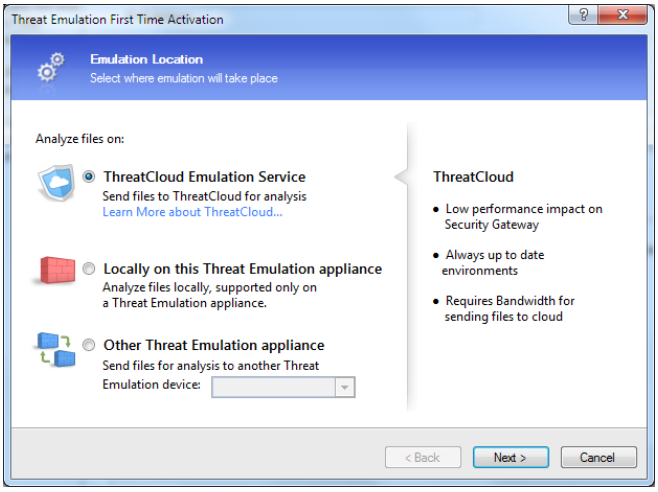
El despliegue podría ser, como hemos dicho antes *inline*, con una copia del tráfico (puerto SPAN), como MTA (protección específica de correo) o como desarrollo propio utilizando APIs. Por último, existe la posibilidad de una integración con un proxy existente utilizando ICAP.

Para su configuración:

– Lo primero es habilitar el *Software Blade* de "Threat Emulation" en el *Security Gateway/Quantum Spark* correspondiente:



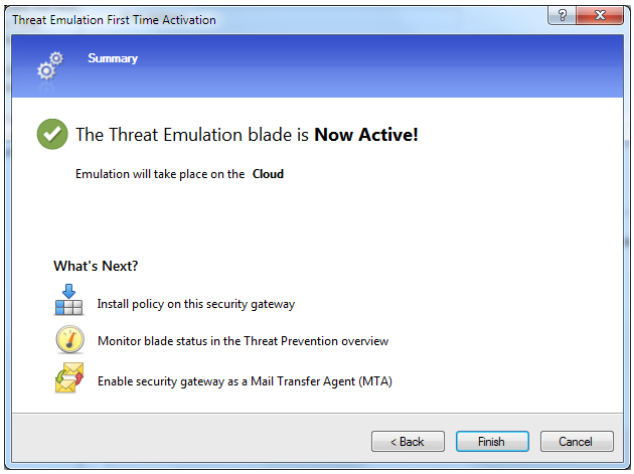
– Seguir el wizard Inicial:



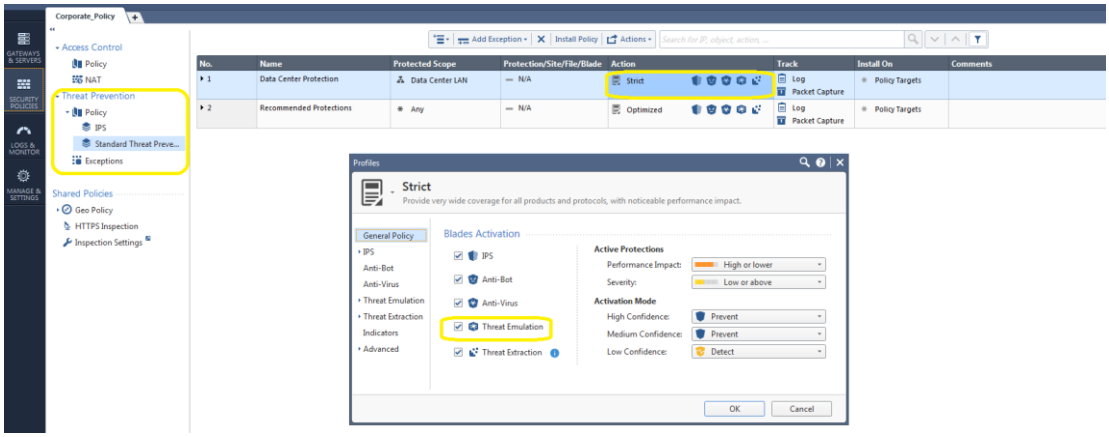
– Hay varias opciones de configuración:

  - Realizar la emulación en *ThreatCloud* enviando los ficheros a emular por SSL.
  - Realizar la emulación localmente en el mismo *appliance*, sólo esta soportada esta opción en *Threat Emulation Appliances*.
  - Realizar la emulación enviando los ficheros a otro *Threat Emulation appliance*, seleccionando el objeto correspondiente en el desplegable.

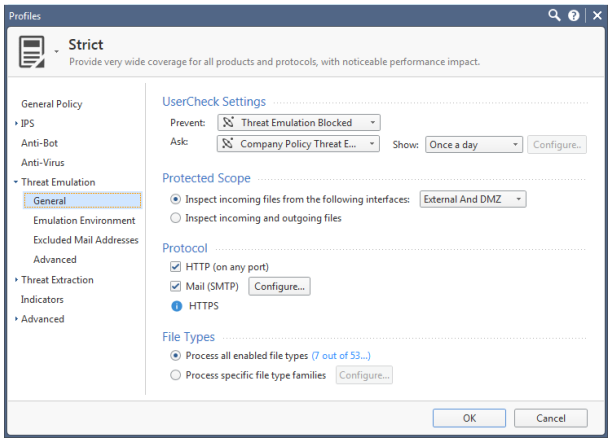
– A continuación se chequeará la salida a internet y el acceso a las actualizaciones y por último quedará activada la funcionalidad.



– El siguiente paso es habilitar el Software Blade en el perfil de las políticas de Threat Prevention:

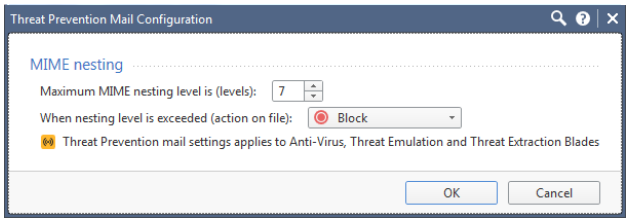


– Navegar a la sección de Threat Emulation:

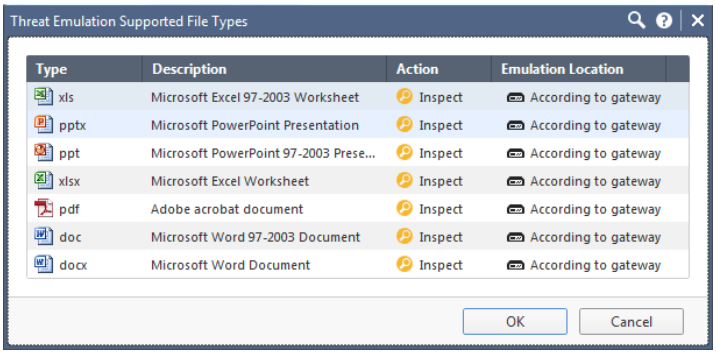


– En “General“, el primer apartado es el de UserCheck para poder definir qué mensajes mostrar al usuario en caso de que se detecte un evento de Threat Emulation.
    - Prevent: Seleccionar el mensaje UserCheck que se abrirá ante un evento cuya acción sea prevenir.
    - Ask: Seleccionar el mensaje UserCheck que se abrirá ante un evento cuya acción sea Ask. Y con qué frecuencia se mostrará el mensaje.
– En la sección “Protected Scope” se definirá tanto el tipo de interfaz como la dirección del tráfico que será protegido.
    - Inspeccionará ficheros entrantes desde las siguientes interfaces:
        - Interfaz externa.
        - Interfaz externa y DMZ.
        - Todas las interfaces.
    - Inspeccionará todos los ficheros entrantes y salientes
– En cuanto a los protocolos sobre los que se aplicará la funcionalidad de Anti-Virus tenemos distintas opciones:
    - HTTP (en cualquier puerto)
    - Mail (SMTP)
    - HTTPS en caso de que se habilite HTTPS Inspection.

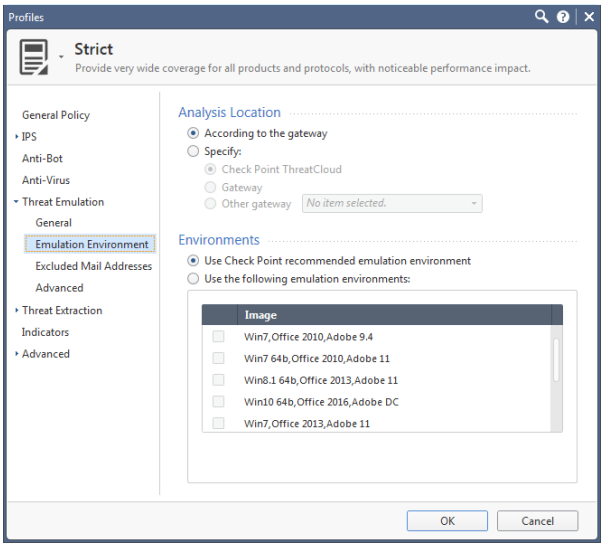
- En caso de proteger SMTP hay varias opciones de configuración:



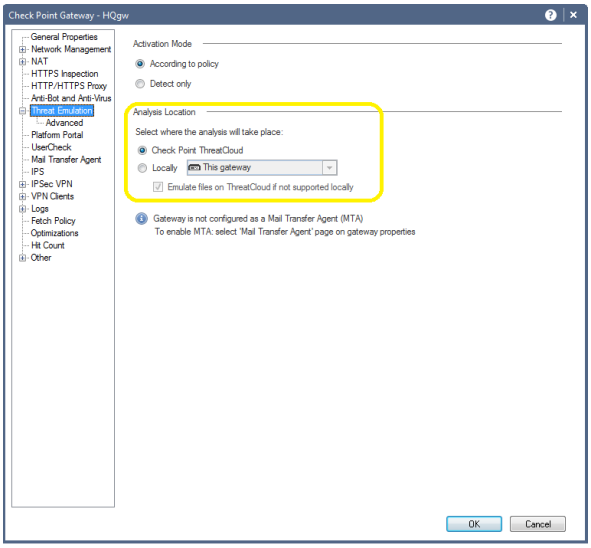
- Configuración de anidamiento MIME: Establece el número máximo de niveles en cuanto al anidamiento MIME que el motor ThreatSpect escanea en el correo electrónico. Cuando se excede el nivel de anidamiento se configura si la acción será bloquear o permitir el archivo.
- También se puede seleccionar el tipo de archivos:
  - Procesar todos los tipos de ficheros habilitados.
  - Configurar la acción que se llevará acabo según el tipo de fichero.



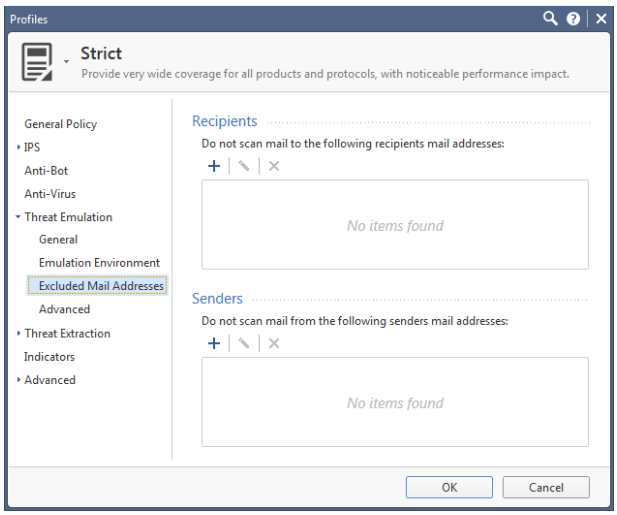
- Se puede configurar la acción que se llevará acabo (Inspect o Bypass) y además donde se emularán dichos ficheros (localmente o en Threat Cloud). En "Emulation Environment":



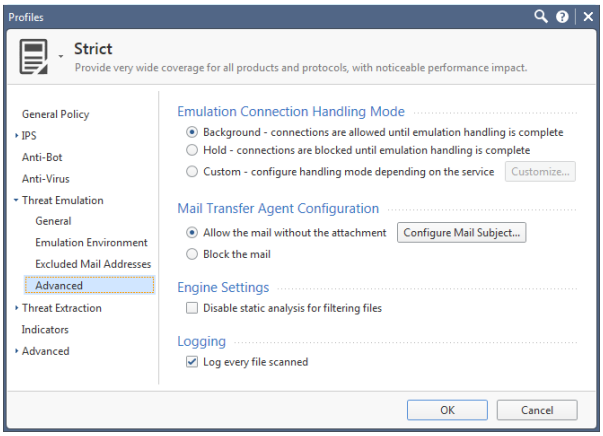
- Lo primero es elegir la localización de la emulación, que se configura en el objeto *Gateway* o especificándolo en el propio perfil *Threat Cloud*, en el propio equipo en un *Threat Emulation Appliance* dedicado)



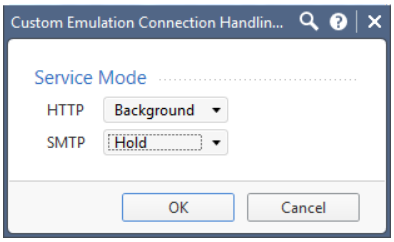
- Por otro lado se elige sobre que imágenes de sistema operativo se va a emular:
  - Emular siguiendo el entorno recomendado por Check Point.
  - Seleccionar sobre cuál o cuáles imágenes queremos emular nuestros ficheros.
- En "*Excluded Mail Address*":



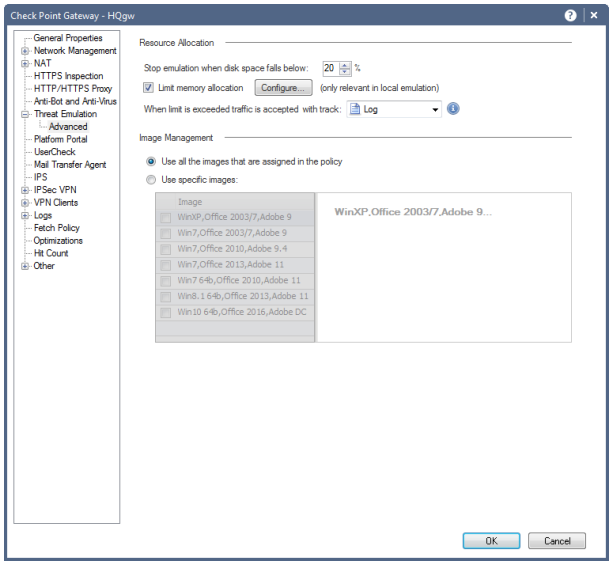
- En este apartado se puede configurar por un lado que emails cuyas direcciones de email de destino que añadamos en el primer apartado no se escanearán y por otro lado que emails cuyas direcciones de email de origen que añadamos en el segundo apartado no se escanearán.
- En "Advanced":



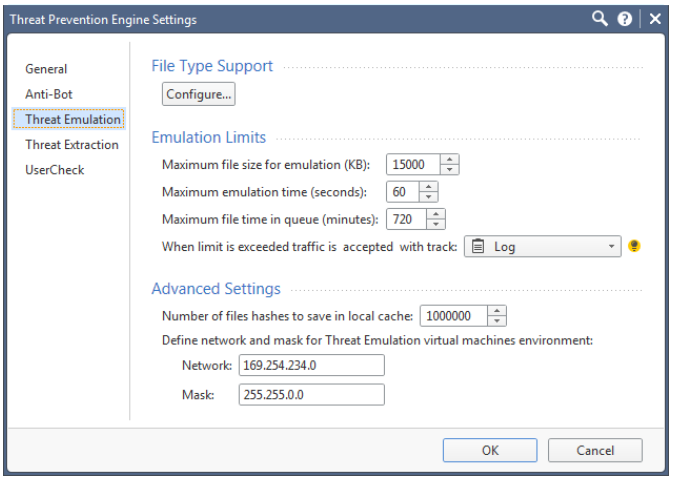
- En el primer apartado se elige el modo de funcionamiento:
  - *Background*: Las conexiones serán permitidas aunque aún se esté realizando la emulación y no se tenga un veredicto.
  - *Hold*: Las conexiones serán bloqueadas hasta que se realice la emulación y se tenga un veredicto.
  - *Custom*: Una combinación de las dos primeras según el protocolo.



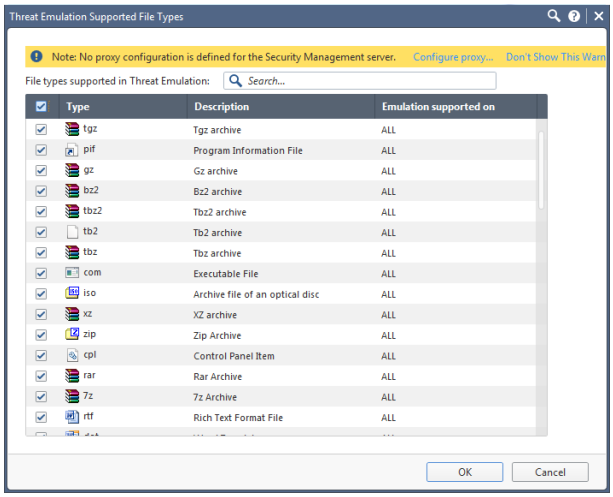
- El segundo apartado está relacionado con el funcionamiento en cuanto al protocolo SMTP:
  - Permite que llegue el correo a su destinatario pero sin el adjunto al detectar un fichero malicioso.
  - Bloquea la recepción del email.
- Asignación de recursos, para poder configurar esta parte es necesario irse al objeto Gateway a la pestaña: Threat Emulation ➔ Advanced.



- En este caso se puede fijar en tanto por ciento de umbral de espacio en disco, si está por debajo de ese umbral se parará la emulación (por defecto el 20%). Y en caso de que se llegue a este límite como poder hacer seguimiento (log, alert, etc).
- Quedaría poder fijar los tipos de ficheros que va a soportar la emulación y los límites de la misma, para ello, en el menú principal “Manage & Settings”, seleccionar “Blades” ➔ “Threat Prevention” y acceder a la sección “Threat Emulation”:



- En un primer momento seleccionar las familias de ficheros que se quieren emular:



- Por otro lado establecer los límites:
  - Máximo tamaño de fichero a emular (por defecto 15000 KB).
  - Máximo tiempo de emulación (por defecto 60 segundos).
  - Máximo tiempo que el fichero puede estar en cola (por defecto 720 minutos).
  - Cuando se excede el límite, el tráfico se deja pasar y se avisa al administrador mediante Log o Alerta.

10.4.2 THREAT EXTRACTION

Threat Extraction proporciona una nueva aproximación a la hora de eliminar el malware contenido en los documentos descargados de la Web y enviados mediante correo electrónico.

Threat Extraction elimina el contenido que puede aprovechar una vulnerabilidad, como las macros, objetos y archivos incrustados, y enlaces externos. Los usuarios reciben los documentos reconstruidos con elementos que se sabe que son seguros.

Soporta los tipos de archivo más comunes usados hoy en día, incluyendo documentos Word, Excel, y Power Point de Microsoft Office, y PDFs de Adobe. Los administradores pueden seleccionar cuáles de estos tipos serán sometidos a *Threat Extraction* cuando entren en la red a través de correo o de descargas Web.

Threat Extraction proporciona varias opciones de protección, la mas recomendable es reconstruir y convertir los documentos a un formato PDF. De modo alternativo, las organizaciones pueden elegir mantener el formato del documento original, y eliminar el contenido que pueda suponer una amenaza.

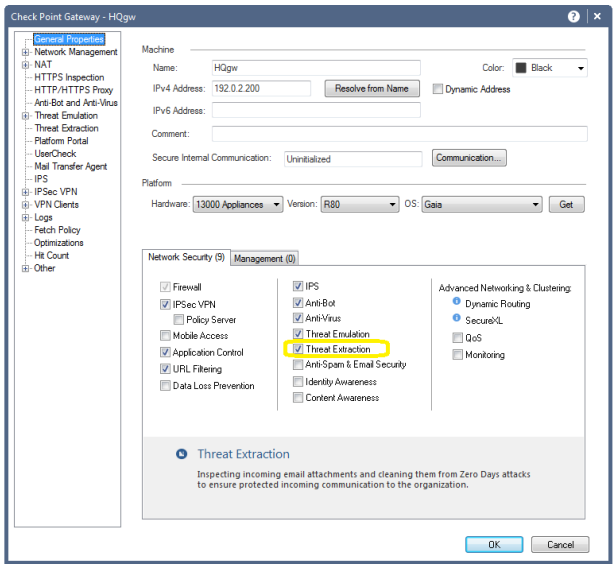
ESPECIFICACIONES

Característica	Descripción
Tipos de archivos soportados	Microsoft Office 2003-2013, Adobe PDF
Opciones de implementación	• MTA – el gateway recibe todo el correo electrónico entrante, y lo reenvía al siguiente salto tras la inspección • WebAPI - envía los archivos a la máquina para su reconstrucción • Web Browser Extension (extensión para el navegador Web) - soporta la reconstrucción para los archivos descargados
Rendimiento	~1% de descenso en el rendimiento con 8000 usuarios
Versión y SO	Desde R77.30 usando SecurePlatform o GAiA

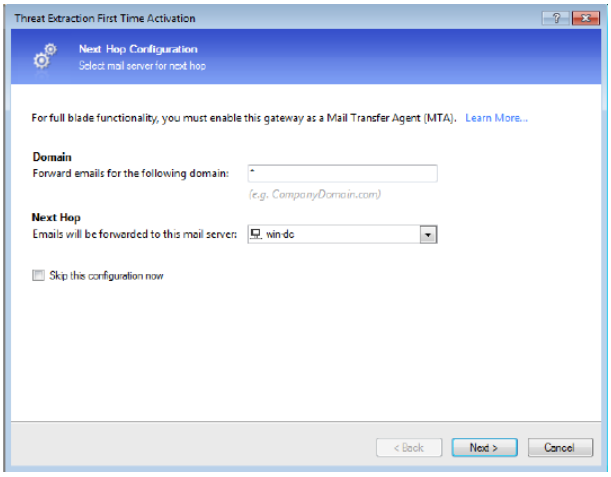
Se puede aplicar *Threat Extraction* en toda la organización, o impleméntelo solo para determinadas personas, dominios o departamentos. Los administradores pueden configurar los usuarios y grupos incluidos basándose en sus propias necesidades, facilitando de una forma sencilla su implementación gradual en la organización.

Para su configuración:

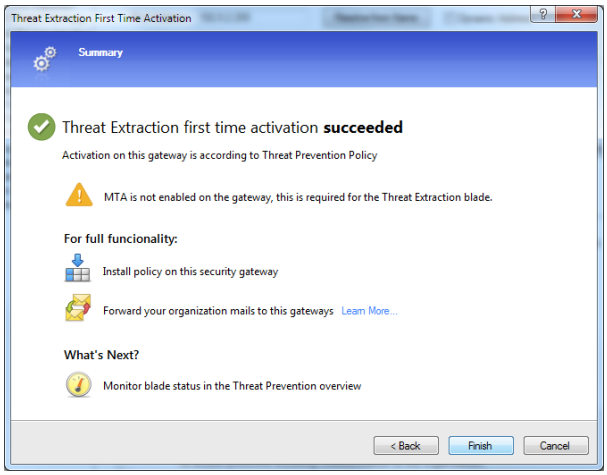
- Lo primero es habilitar el *Software Blade* de *Threat Emulation* en el *Security Gateway/Quantum Spark* correspondiente:



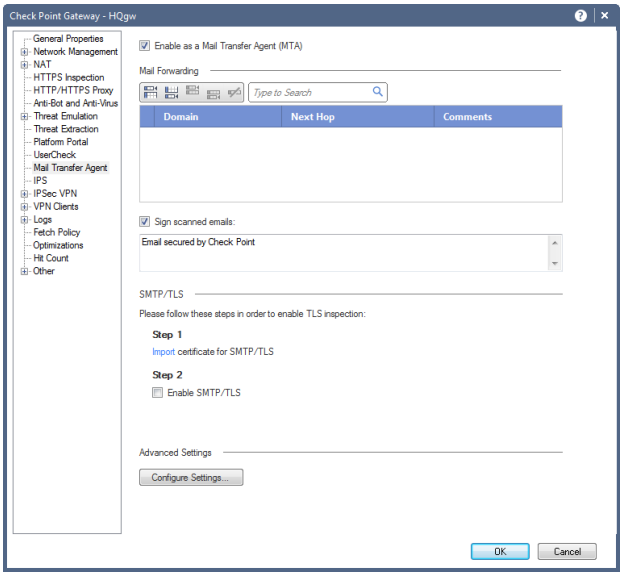
- Seguir el wizard Inicial:



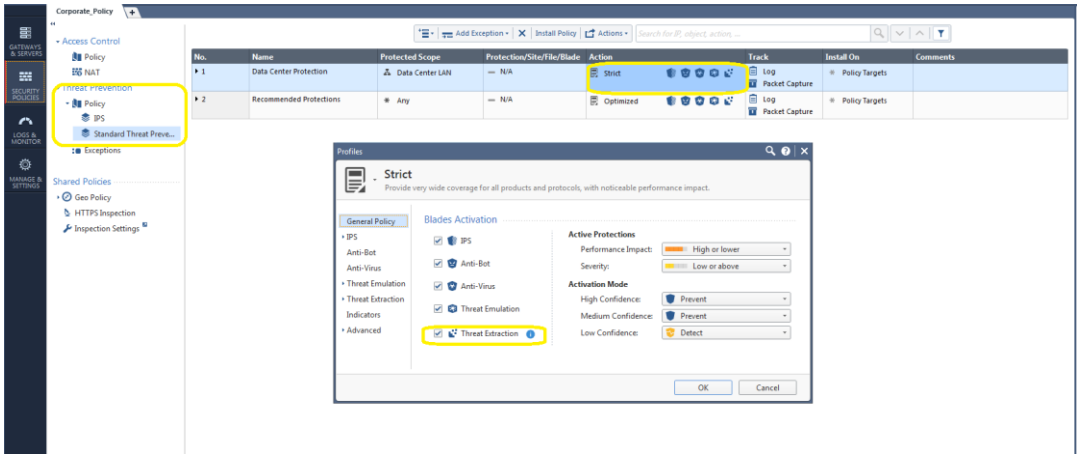
- Para habilitar *Threat Extraction* en el correo electrónico es necesario configurar el *Gateway* como *Mail Transfer Agent* (MTA).
- Lo primero es fijar el dominio y el siguiente paso, es decir el servidor de mail al que serán redirigidos los correos.



- Configurar como MTA: Para una topología que usa TLS entre *Security Gateway/Quantum Spark* y el servidor de correo, debe importar el certificado del servidor de correo al *Security Gateway*. Lo primero es en el objeto *Gateway* seleccionar “Mail Transfer Agent”:

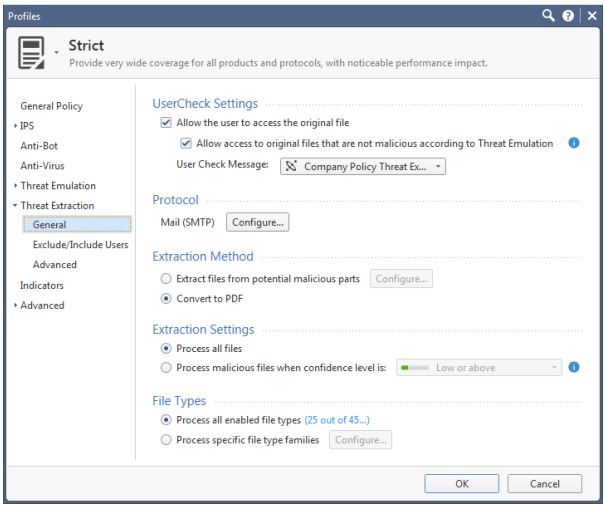


- Seleccionar “Habilitar” como MTA, y en la sección de “Reenvío” de correo, agregar una o más reglas, basándose en el dominio y el *next hop* o servidor de correo al que redirigir los correos electrónicos.
- Si el servidor de correo usa la inspección TLS, es necesario importar el certificado (Paso 1) e introducir la contraseña de la clave privada para el certificado. Y Como último paso (Paso 2) seleccionar “Habilitar SMTP/TLS”.
- Después de configurar *Security Gateway/Quantum Spark* como MTA, cambie las configuraciones para enviar tráfico SMTP desde redes externas al *Security Gateway*. Cada organización tiene un registro MX que apunta al servidor de correo interno, o un MTA diferente. El registro MX define el siguiente salto para el tráfico SMTP que se envía a la organización. Estos procedimientos explican cómo cambiar las configuraciones de red para enviar SMTP al MTA de Check Point.
- El siguiente paso es habilitar el *software blade* en el perfil de las políticas de *Threat Prevention:*

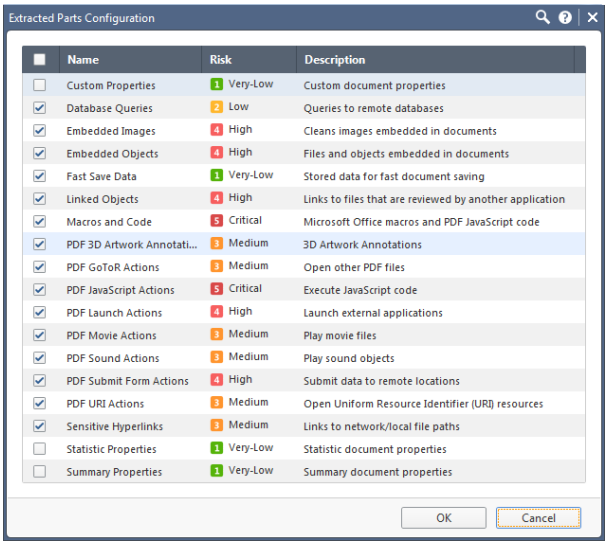


- Navegar a la sección de *Threat Extraction*:

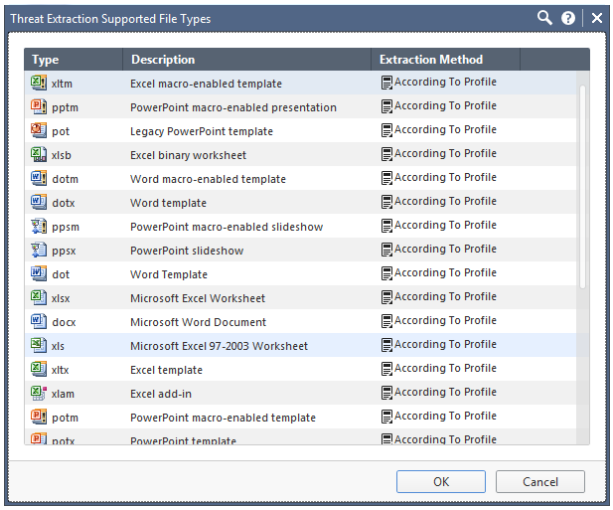
  En “General”:



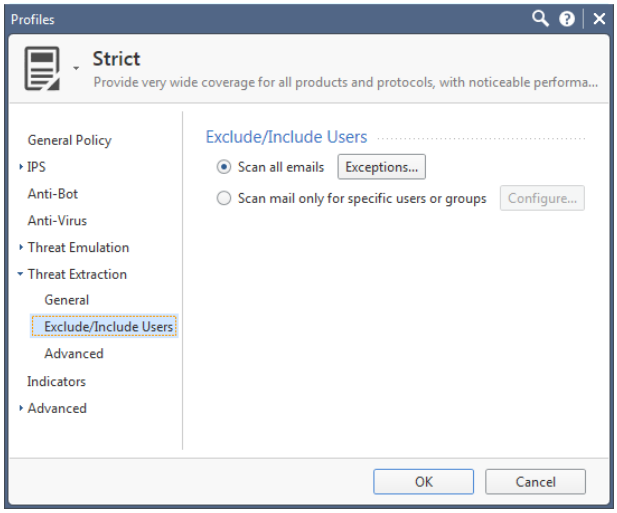
- El primer apartado es el de *UserCheck* para poder definir qué mensajes mostrar al usuario en caso de detectar un evento de *Threat Extraction*.
    - Permitir que el usuario acceda al fichero original cuyo veredicto al pasar por *Threat Emulation* es benigno.
    - Message: Seleccionar el mensaje *UserCheck* que se abrirá ante un evento de *Threat Extraction*.
- Lo siguiente es el protocolo sobre el que se va a realizar: SMTP o HTTP.
- Después en "*Extraction Method*", elegimos si vamos a convertir el fichero a PDF o mantener su formato original y eliminar cualquier componente activo.



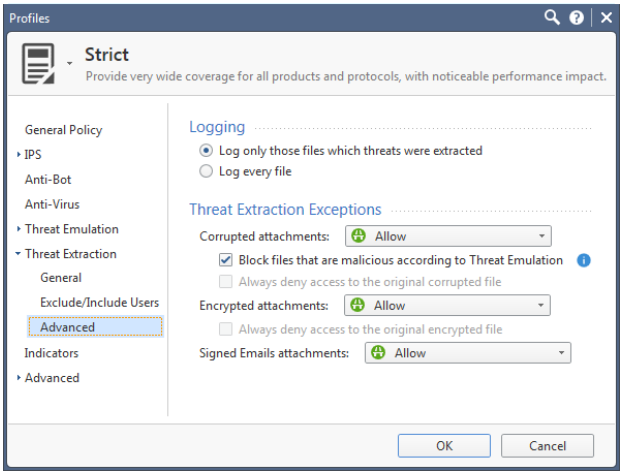
- En la sección "*Extraction Settings*", se configura si se van a procesar todos los ficheros o según su nivel de confianza:



– En “Exclude/Include Users”:

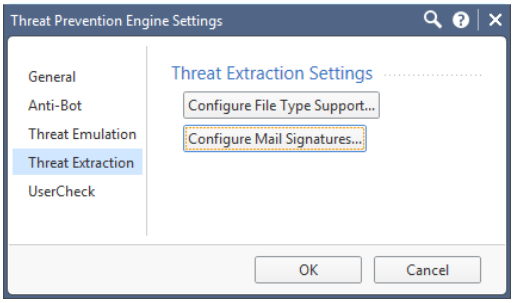


– Se puede escanear todos los correos electrónicos añadiendo excepciones manualmente o escanear sólo específicos usuarios o grupos. En “*Advanced*”:

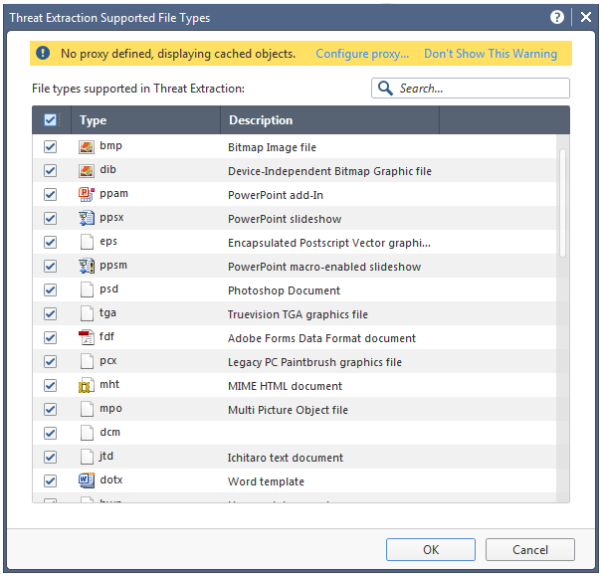


– La primera sección está relacionada con los *logs*, se genera un *log* por cada fichero en el que las amenazas fueron extraídas o se genera un log por fichero. Luego tomamos decisiones si por ejemplo los adjuntos de los mails están corruptos, encriptados o están firmados.

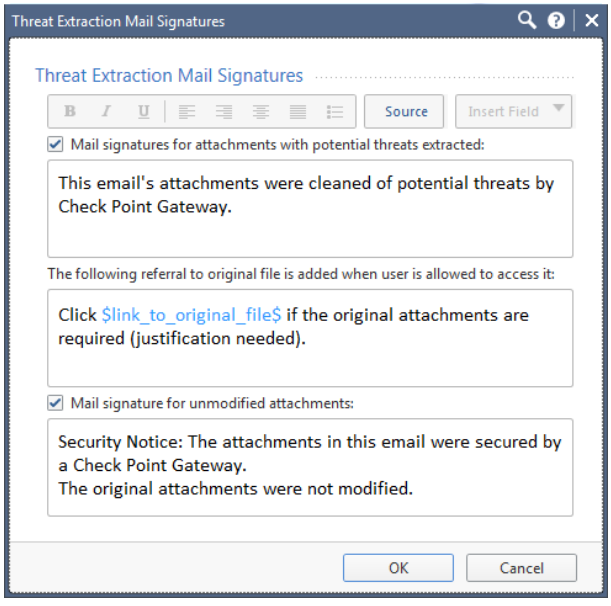
– Por último, quedaría fijar los tipos de ficheros que va a soportar la extracción y customizar las firmas en los correos electrónicos, para ello, en el menú principal "Manage & Settings", seleccionar *Blades* ➔ *Threat Prevention* y acceder a la sección "Threat Extraction":



– Primero es elegir los ficheros soportados:



– Y para finalizar personalizamos las firmas que se mostrarán en los correos electrónicos:



11. FUNCIONALIDADES DE GESTIÓN

SmartConsole es una solución integrada de administración de seguridad que incluye políticas, registros, monitorización, correlación de eventos e informes, todo en un solo sistema que permite a los administradores identificar fácilmente los riesgos de seguridad en toda la organización.

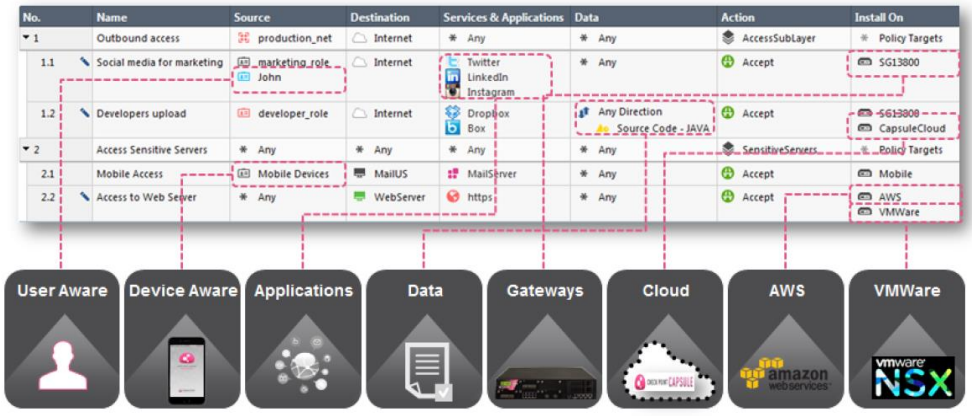
Además permite que varios administradores trabajen simultáneamente en el mismo servidor de administración, o incluso en la misma política sin conflictos. También permite la delegación de tareas rutinarias, para que los equipos puedan centrarse mejor en la supervisión y la respuesta a incidentes.

11.1 SERVIDOR DE GESTIÓN (SMS)

La gestión y administración de los *Gateways* de Check Point se realiza de forma centralizada mediante el *blade* de *Network Policy Management* (NPM). La gestión centralizada permite obtener una visibilidad completa de las políticas y accesos, rendimiento de los recursos en los *Gateways*, túneles VPN, usuarios remotos, etc.

Un administrador puede agregar licencias al repositorio central y asignar esas licencias a los componentes según sea necesario, incluso actualizar paquetes software e instalar archivos de contrato.

La administración unificada tanto para redes físicas como virtuales, despliegues en la nube como en instalaciones físicas, asegura la consistencia de la seguridad y la visibilidad total del tráfico en la red.



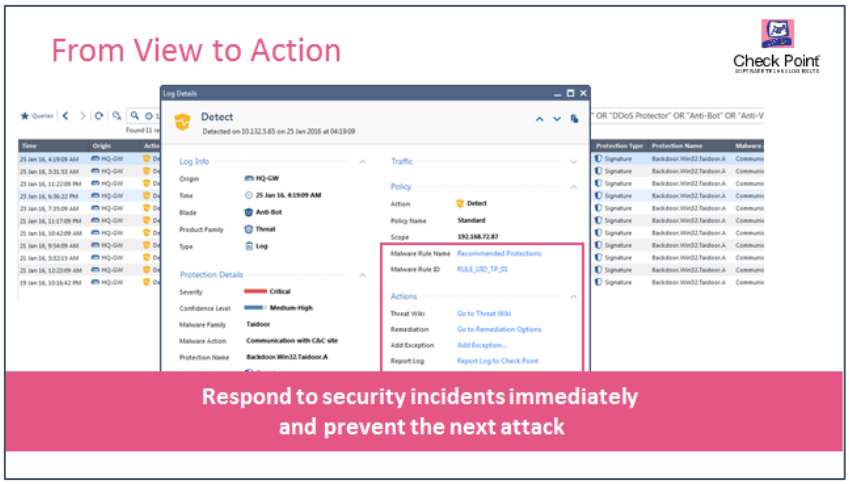
El primer punto destacado es la granularidad en la gestión de políticas, diferenciando reglas relacionadas con el control de acceso y reglas relacionadas con el control de seguridad.

Check Point segmenta la política en secciones. A esta solución se le conoce como *Multi-Layer* ya que las políticas utilizadas están compuestas por capas. Cada capa o subpolítica se puede delegar, automatizar o implementar de forma independiente. Con API R81, se pueden automatizar cualquier tarea o crear una serie de portales para el autoservicio de seguridad.

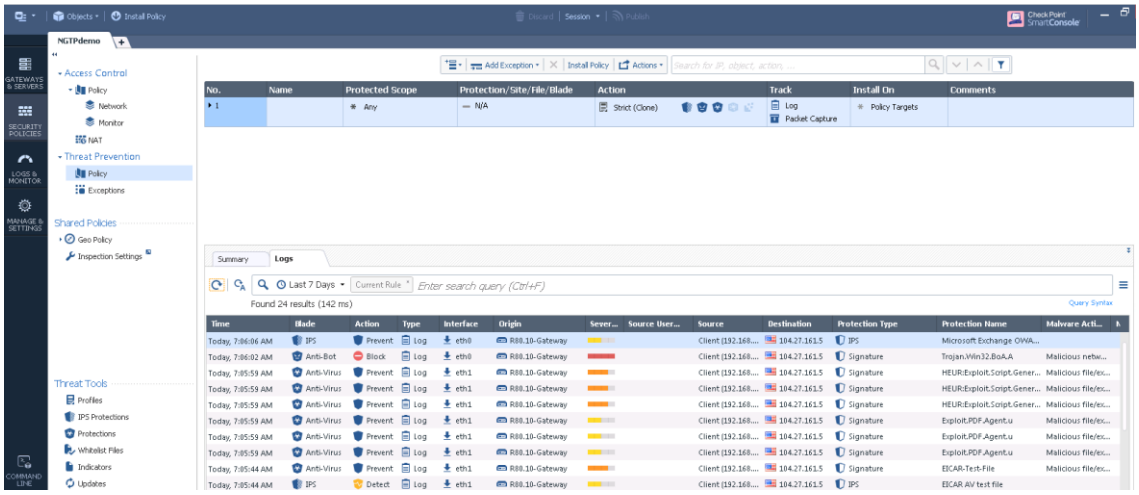
La administración concurrente permite que varios administradores trabajen simultáneamente en la misma política sin conflictos.

Un panel de control visual proporciona una visibilidad de la seguridad en toda la red, lo que le ayuda a controlar el estado de sus puntos de cumplimiento y a estar alerta ante posibles amenazas.

Además existe la herramienta de *SmartLog*, que nos facilita información en tiempo real, ya sea a nivel global o haciendo nuestras propias búsquedas.



Este tipo de logs podemos visualizarlos desde el apartado exclusivo para *logs/reporting* o ubicándonos encima de una regla, dado que en la parte inferior se muestran los logs referenciados a dicha regla.



11.2 SMARTEVENT

La seguridad actual es compleja y requiere múltiples dispositivos que generan voluminosas cantidades de registros. Un sistema de detección de intrusos puede producir más de 500,000 mensajes por día y los cortafuegos generar millones de registros diarios.

No es humanamente posible escanear toda esta información e incluso con el análisis de registro automatizado, lleva mucho tiempo identificar incidentes críticos de seguridad e investigarlos. Lo que puede parecer un comportamiento normal cuando se visualiza por sí solo, puede revelar evidencia de actividad anormal cuando esos datos están correlacionados y analizados.

Uno de los puntos más relevantes a la hora evaluar una consola de administración es la herramienta de reporting/log que lleva.

La solución presentada está formada por dos herramientas de reporting/logs con dos objetivos diferentes:

- Análisis de *logs* haciendo uso de información facilitada
- Foto de la situación actual

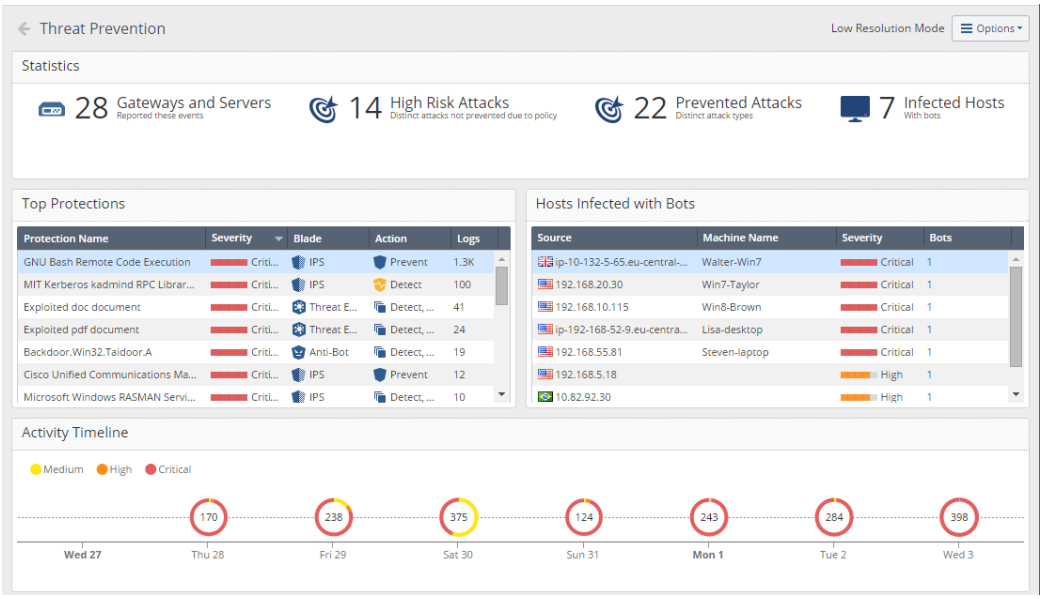
En cualquier escenario de gestión se precisa de una herramienta que facilite la búsqueda de información de eventos sobre un base de datos, ofreciendo el resultado de la búsqueda de una forma clara y concisa. *SmartEvent* es la herramienta de gestión y correlación de Eventos de Check Point que automatiza la agregación y la correlación de los datos de registro, y los patrones de ataque potenciales.

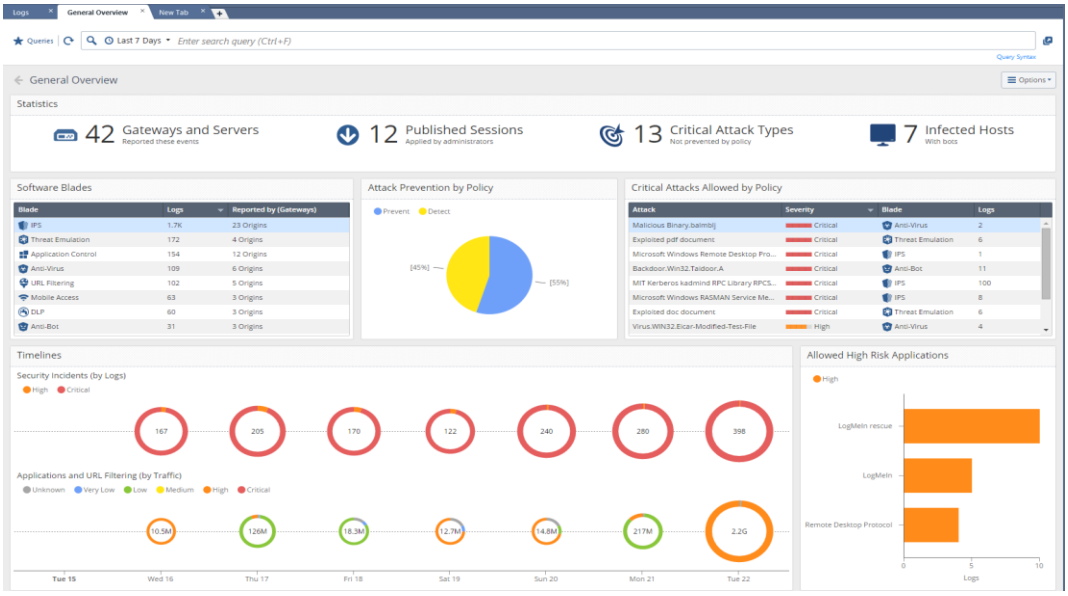
SmartEvent también consolida funciones de monitorización, registro, informes y análisis de eventos dentro de la misma consola. Esto significa que puede pasar de rastrear tendencias a investigar eventos mediante búsqueda de texto libre.

Una vez que investigado un evento, es fácil actuar sobre él. Dependiendo de la gravedad del evento, puede optar por ignorarlo, actuar sobre él más tarde o bloquearlo de inmediato. También puede aprovechar eventos de seguridad predefinidos o personalizarlos para priorizar eventos, configurando alertas automáticas.

SmartEvent es un *Software Blade* con licencia y se puede instalar en un único servidor o en varias unidades de correlación para reducir la carga de la red.

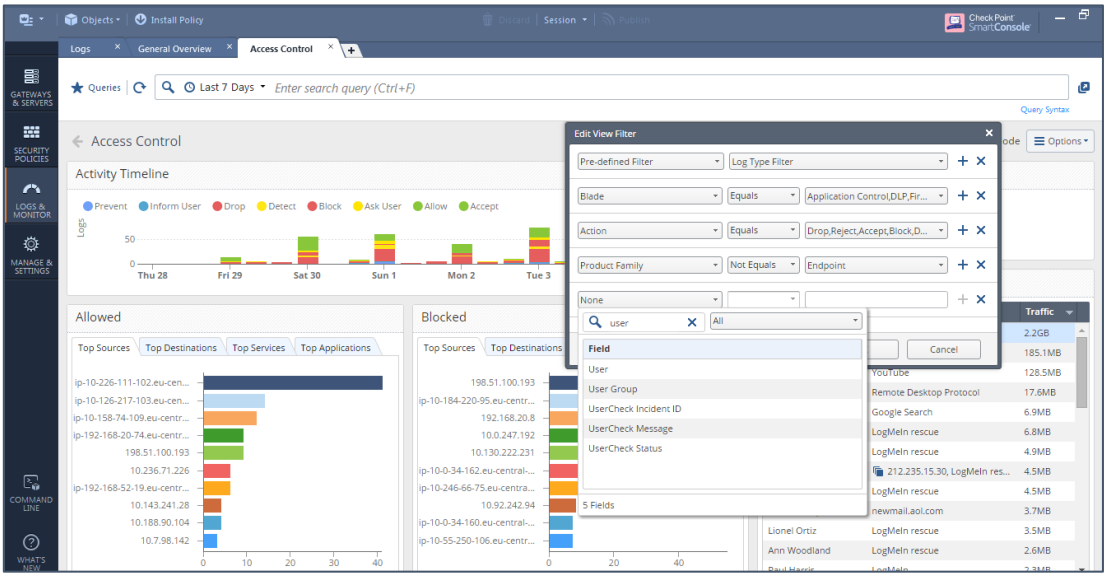
Las vistas de *SmartEvent* se pueden personalizar para supervisar los patrones y eventos que son más importantes. La información se puede mostrar desde una vista de alto nivel hasta una vista detallada a nivel de análisis forense. Los *widgets* y las plantillas de gráficos optimizan la visualización. Con el motor de búsqueda de texto libre se pueden ejecutar análisis de datos e identificar eventos críticos de seguridad.

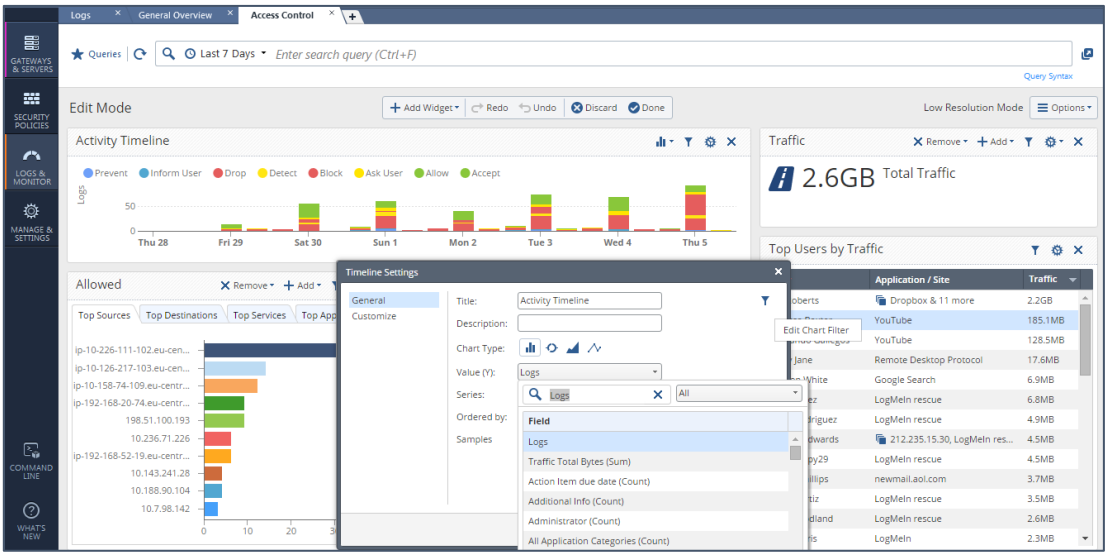




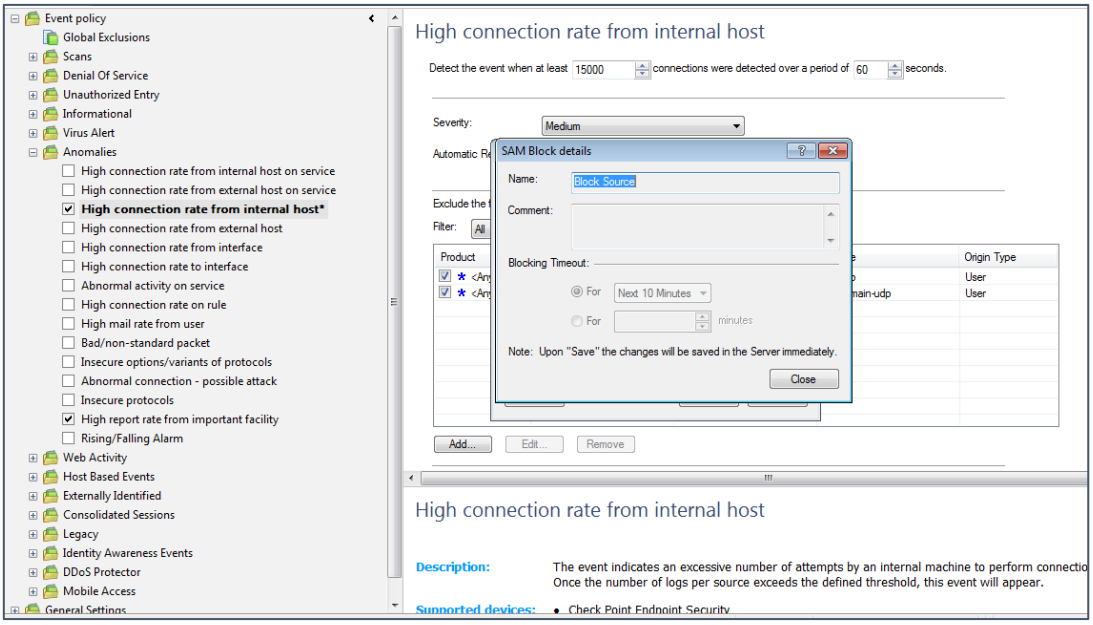
Si nos centramos en la funcionalidad de reporting, Check Point nos proporciona una herramienta integrada que representa de una forma gráfica los eventos que ha cursado la solución de seguridad.

Se trata de una herramienta configurable, donde se presentan una serie de vistas predefinidas y el administrador puede escoger que representar y el formato de representación:

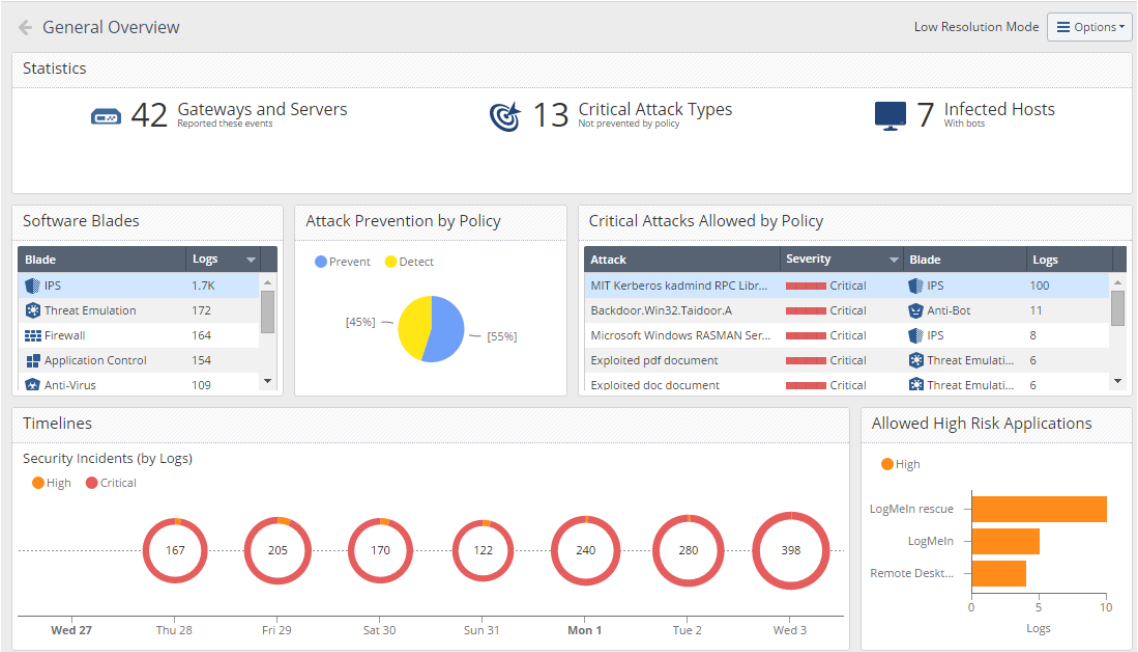




SmartEvent facilita la personalización de informes para las diferentes partes interesadas en una organización. La herramienta no solo transforma las entradas en los *logs* en eventos, sino también es capaz de hacer uso del módulo de correlación para obtener respuestas automáticas frente a eventos específicos.



El portal web *SmartView* proporciona acceso a informes y datos de panel a través de teléfonos móviles y tabletas, accediendo por HTTPS a la IP de la gestora usando un navegador:



11.3 COMPLIANCE

Las organizaciones de hoy en día necesitan saber si su arquitectura de seguridad se define de acuerdo con las mejores prácticas con el fin de identificar las debilidades de las políticas y de su configuración. Los entornos de seguridad deben cumplir con las políticas y regulaciones.

Compliance Software Blade se encarga de escanear continuamente las configuraciones de políticas y configuraciones, resaltando todas las debilidades y errores de configuración, y poniéndolos a disposición para su corrección. Gracias a esto, se puede saber si la configuración actual es la mejor posible. La monitorización se realiza 24/7 y permite enviar alertas en tiempo real en caso de incumplimientos.

Además incluye una biblioteca de mejores prácticas de seguridad que permite a las organizaciones monitorizar y comparar el entorno de Check Point con las recomendaciones de seguridad. Las organizaciones pueden crear sus propias Políticas de buenas prácitcas de seguridad personalizadas como parte de la supervisión y análisis continuos.

Las alertas de seguridad en pantalla y los informes de cumplimiento predefinidos permiten a las organizaciones reducir el tiempo y costes asociados con el mantenimiento de la seguridad optimizada y la preparación de auditorías. Esto, a su vez, libera recursos para enfocarse en la administración de la seguridad.

Con cada mejor práctica de seguridad, surgen las recomendaciones correspondientes, que ayudan a comprender cómo mejorar el cumplimiento y la seguridad.

Además las alertas de seguridad automatizadas permiten saber de inmediato cuando las violaciones afectan negativamente su estado general de seguridad, ocurriendo justo después de guardar un cambio en la política, lo que significa que no es necesario instalar la política de seguridad primero. Esto reduce el tiempo asociado con la administración de cambios y minimiza los errores.

11.4 MULTIDOMAIN MANAGEMENT (MDM)

La solución *MultiDomain Management* es una administración centralizada para entornos distribuidos a gran escala, con muchos segmentos de red distintos, cada uno con diferentes requisitos de seguridad. Esta solución permite a los administradores crear dominios basados en la geografía, unidades de negocios o funciones de seguridad para fortalecer la seguridad y simplificar la administración.

Cada dominio tiene sus propias Políticas de seguridad, objetos de red y otras configuraciones. Utiliza el dominio global para las Políticas de seguridad comunes que se aplican a todos o a los dominios especificados. El dominio global también incluye objetos de red y otras configuraciones que son comunes a todos o a los dominios especificados.

Un servidor multidominio es un servidor físico que contiene los servidores de dominio, las Políticas de seguridad, los datos del sistema y el software del *Multidomain Management*. Se conecta a un servidor multidominio para trabajar con funciones, objetos y ajustes de administración de multidominio. Esto incluye:

- Servidores de dominio y sus configuraciones.
- Políticas globales y objetos.
- Administradores y perfiles de permisos.
- Registros y funciones de monitorización.
- Configuración del sistema.

Puede crear una implementación de alta disponibilidad y compartir carga con dos o más *Multidomain Server*.

Un dominio (Domain server) es un objeto virtual que define una red o una colección de redes relacionadas con una entidad. Puede definir un dominio para una organización, departamento, sucursal o ubicación geográfica.

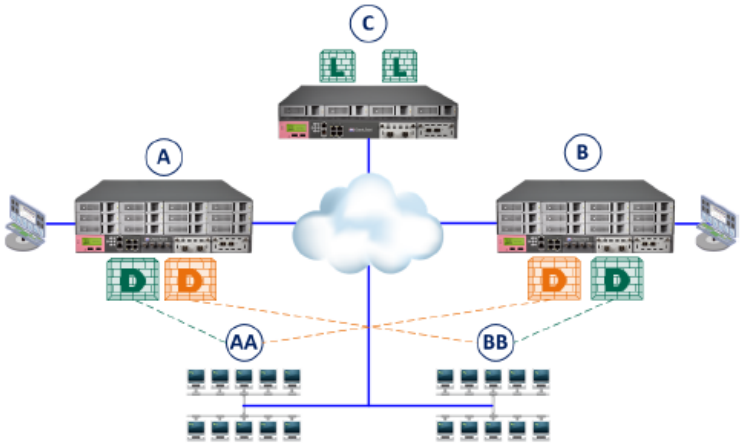
Un servidor de dominio es el equivalente funcional de un Servidor de administración de seguridad en un entorno de dominio único. Se conecta directamente a un servidor de dominio con *SmartConsole* para administrar un dominio y sus componentes:

- Domain security gateways.
- Domain security Policicies, reglas y otras configuraciones de seguridad a nivel de dominio.
- Domain system objects, como servicios, usuarios y Comunidades VPN.
- Domain software blades y sus configuraciones.

Puede haber más de un *Domain Server* para un determinado dominio en una implementación de alta disponibilidad, cada uno en un *MultiDomain Server* diferente. Un servidor de dominio está activo y el otro servidor de dominio totalmente sincronizado está en modo de espera.

Domain Log server es una implementación típica de administración de varios dominios que incluye, al menos, un servidor de registro multidominio para contener los archivos de registro generados por los *Domain Security Gateways*. Cada dominio puede tener su propio servidor de registro en el *MultiDomain Log Server*. Esta estrategia de despliegue mantiene el tráfico de *logs* aislado de otro tráfico de red para un mejor rendimiento.

Esta ilustración muestra una implementación de muestra con dos Servidores multidominio y dos Dominios. El *MultiDomain Log Server* contiene dos servidores de registro de dominio, uno para cada dominio.



A	London Multi-Domain Server with an Active Domain Server for London and a Standby Domain Server for Tokyo
AA	London network
B	Tokyo Multi-Domain Server with an Active Domain Server for Tokyo and a Standby Domain Server for London
BB	Tokyo network
C	Multi-Domain Log Server with Domain Log Servers for London and Tokyo
	Active Domain Server
	Standby Domain Server
	Domain Log Server

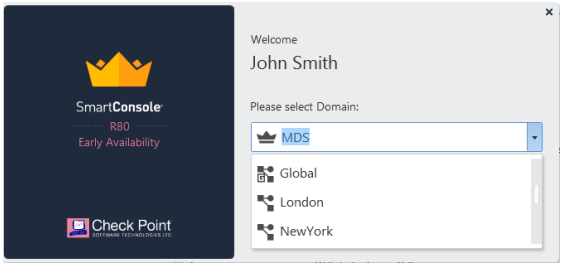
Use *SmartConsole* para conectarse a un *MultiDomain Server* cuando trabaje con objetos y configuraciones de administración multidominio. Use *SmartConsole* para conectarse a un *Domain Server* cuando trabaje con las Políticas de seguridad de las reglas, los objetos y la configuración de un dominio.

Para conectarse a un *MultiDomain Server*:

- Ejecute SmartConsole.
- Ingrese su nombre de usuario y contraseña.
- Ingrese la dirección IP del servidor multidominio y luego pulse en Iniciar sesión.
- En la pantalla de bienvenida, seleccione MDS de la lista y luego pulse en Continuar.

SmartConsole se abre en la vista de Dominios. Para conectarse directamente a un dominio:

- Ejecute SmartConsole.
- Ingrese su nombre de usuario y contraseña.
- Ingrese la dirección IP del servidor multidominio y luego pulse en Iniciar sesión.
- En la pantalla de bienvenida, seleccione un dominio de la lista y luego pulse en Continuar.



Para conectarse a un servidor de dominio desde la vista de *SmartConsole Multi-Domain*:

- Conéctese a un servidor de dominio múltiple con SmartConsole.
- En la vista Multi-Domain➔ Domains, pulse con el botón derecho en el Servidor de dominio activo.
- Seleccionar Conectarse al servidor de dominio.

Nota: en una implementación de alta disponibilidad solo puede realizar cambios en un dominio desde el servidor de dominio activo que se muestra con un icono negro. Si se conecta a un servidor de dominio en espera (icono blanco), SmartConsole se abre en el modo de solo lectura.

La vista "Gateways & Servers" muestra todos los objetos *Security Gateway, Domain Server* y *Domain Log Server* en el entorno de administración de varios dominios. Esta característica permite a los administradores, con permisos aplicables, ver y trabajar con ellos en una ubicación conveniente.

Puede pulsar dos veces en un objeto en esta vista para abrir su ventana de configuración. Por ejemplo, si pulsa dos veces en GW105 en el siguiente ejemplo, se abre el Servidor de dominio London_Server en SmartConsole y se muestra la ventana de configuración de GW105.

Status	Name	Domain	IP	Version	Active Blades	Hardware
–	GW105	London	192.168.3.105	R77.20	...	4000 Appliances
–	GW106	NewYork	192.168.3.106	R77.20	...	12000 Appliances
–	GW107	Tokyo	192.168.3.107	R77.20	...	13000 Appliances
–	GW115	London	192.168.3.115	R77.30	...	21000 Appliances
–	GW116	NewYork	192.168.3.116	R77.30	...	13000 Appliances
–	GW117	Tokyo	192.168.3.117	R77.30	...	61000 Appliances
–	London_Server	London	192.168.3.150	R80		Open server
–	London_Server_2	London	192.168.3.161	R80		Open server
–	London_Server_3	London	192.168.3.170	R80		Open server
–	London_Server_4	London	192.168.3.130	R80		Open server
–	New_York_Server	NewYork	192.168.3.160	R80		Open server
–	NewYork_Server	NewYork	192.168.3.151	R80		Open server
–	NewYork_Serve...	NewYork	192.168.3.171	R80		Open server
–	NewYork_Serve...	NewYork	192.168.3.131	R80		Open server
–	Tokyo_Server	Tokyo	192.168.3.152	R80		Open server
–	Tokyo_Server_2	Tokyo	192.168.3.162	R80		Open server
–	Tokyo_Server_3	Tokyo	192.168.3.172	R80		Open server
–	Tokyo_Server_4	Tokyo	192.168.3.132	R80		Open server

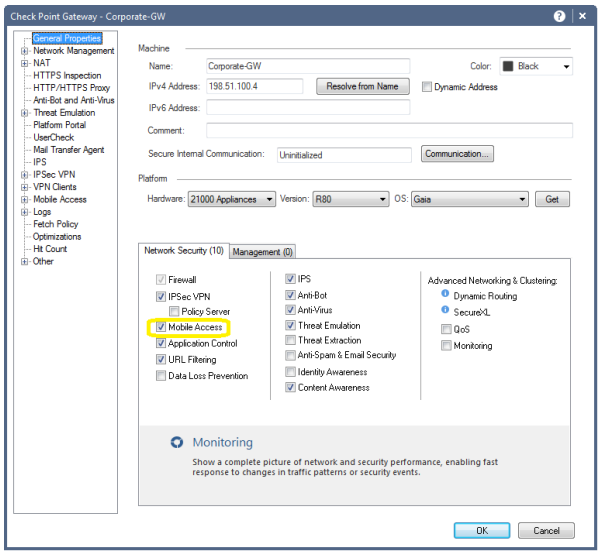
12. SEGURIDAD EN ENTORNOS DE MOVIBILIDAD

Mobile Access es la solución de Check Point para conectarse a aplicaciones corporativas a través de Internet mediante un dispositivo móvil. La solución proporciona acceso remoto a través de VPN de nivel 3 y SSL/TLS.

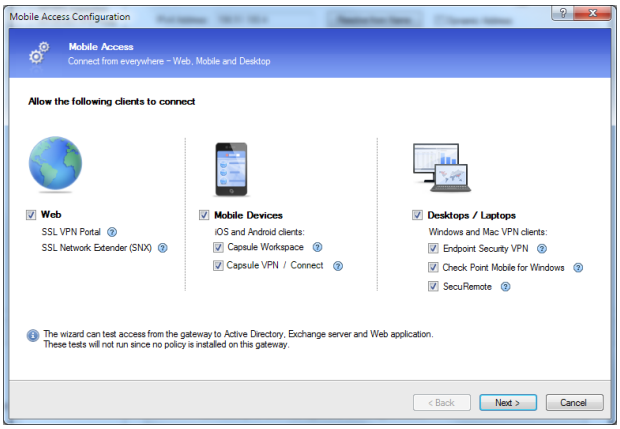
La solución ofrece múltiples opciones de conectividad realizando la autorización de usuarios mediante autenticación de dos factores y emparejamiento de usuario-dispositivo.

Para su configuración:

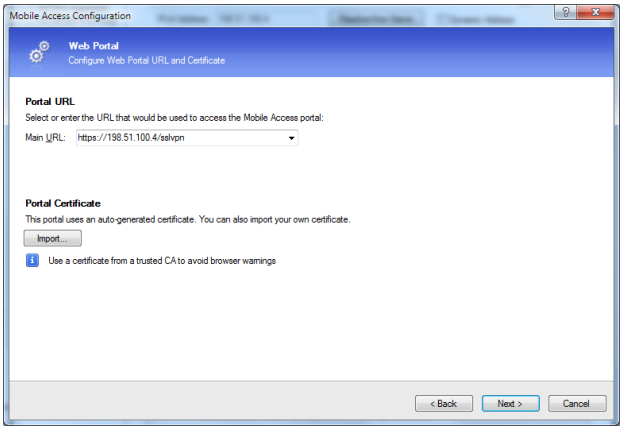
- Lo primero es habilitar el *Software Blade* de "Mobile Access" en el *Security Gateway/Quantum Spark* correspondiente:



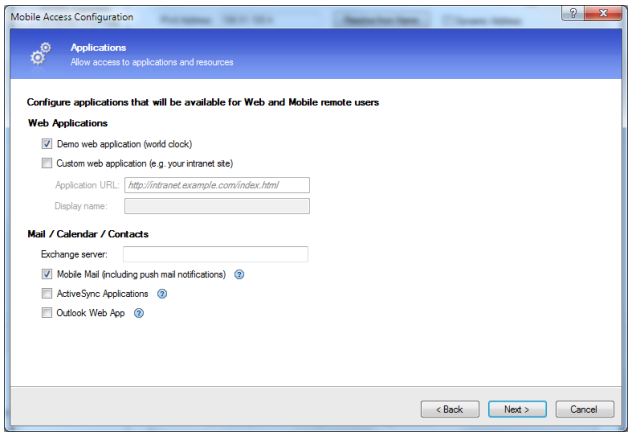
- Seguir el wizard inicial:



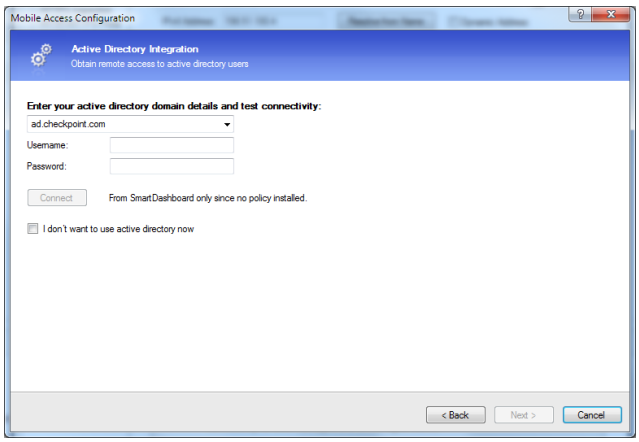
- Configurar desde que entornos queremos hacer accesible los recursos internos:
  - Web
  - Dispositivos móviles (container Workspace o de la propia aplicación de VPN)
  - Desktops/Laptops (Windows y MAC)



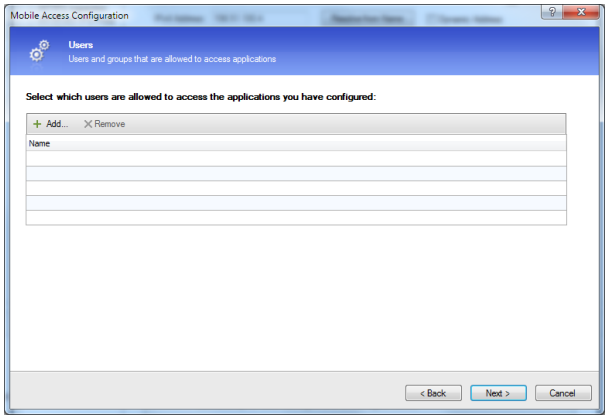
– Establecer la URL de Acceso a la VPN SSL y la posibilidad de importar un propio certificado.

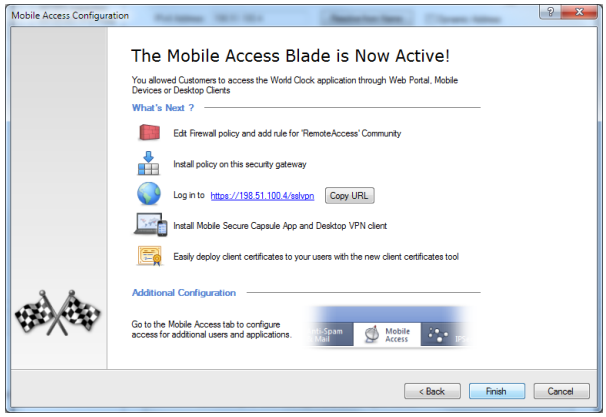


– Configurar que aplicaciones estarán disponibles para los usuarios remotos (a través de URL) y si además vamos a publicar otras aplicaciones como el OWA, *ActiveSync*, etc, es necesario definir el servidor de *Exchange*.

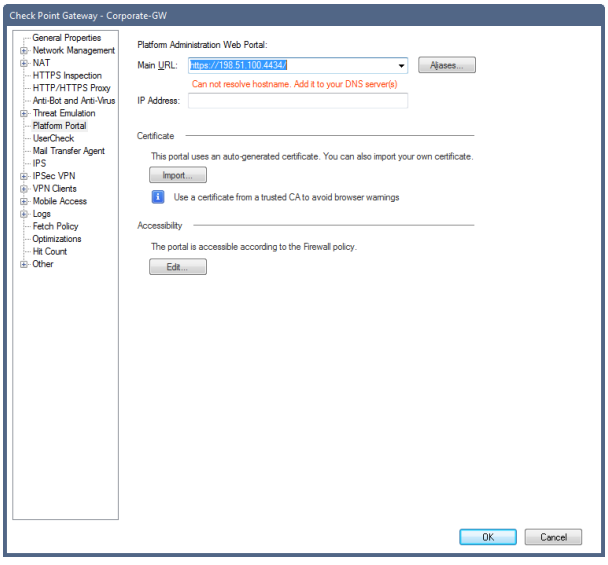


– El siguiente paso es configurar el directorio activo y testear su conectividad (usuario y password de administrador) para poder utilizar grupos de usuarios en las políticas de *Mobile Access*.

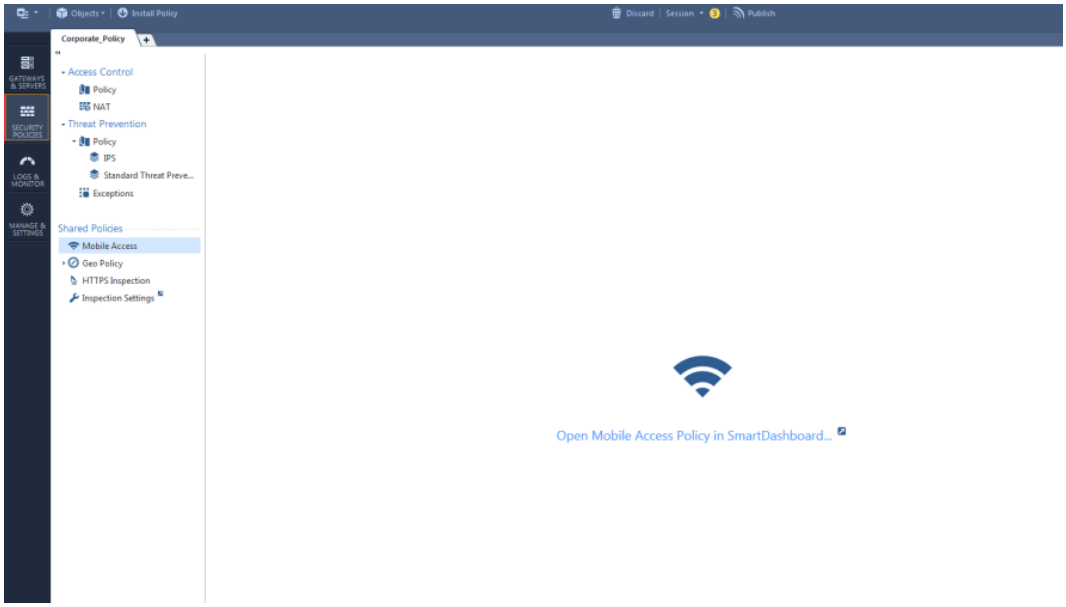




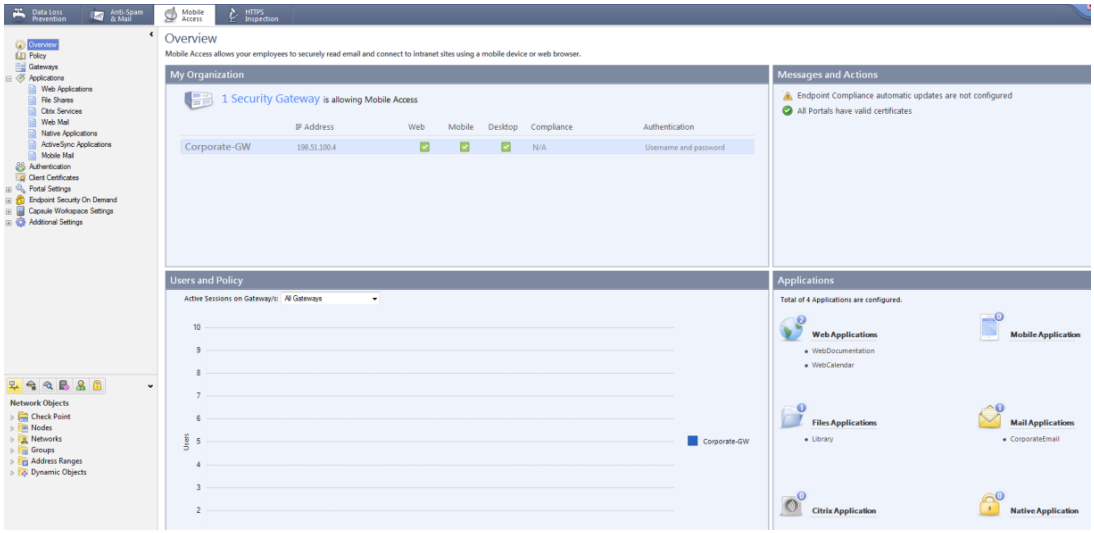
– Es necesario modificar el puerto de acceso al portal Gaia del *Gateway* para que no haya solape con el acceso web a la VPN (por ejemplo usar el puerto 4434). Editar objeto *Gateway* y dentro del menú seleccionar "*Platform Portal*".



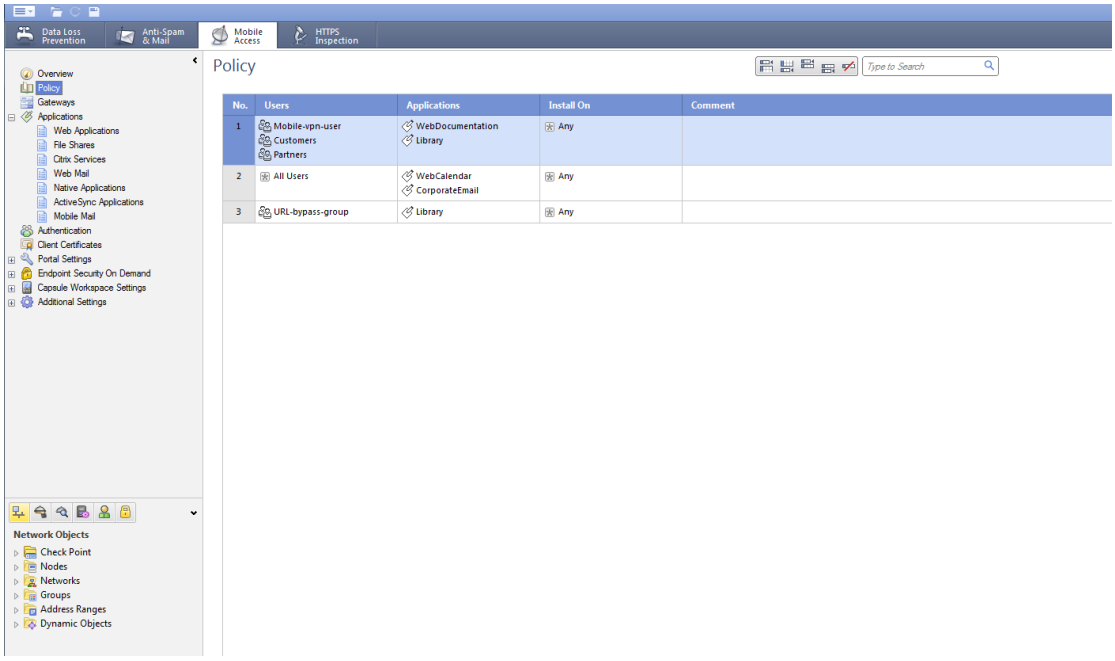
– Para poder ver, modificar y crear las reglas de Mobile Access, es necesario ir a la pestaña de "*Security Policies*" y dentro del menú "*Shared Policies*" elegir "Mobile Access".



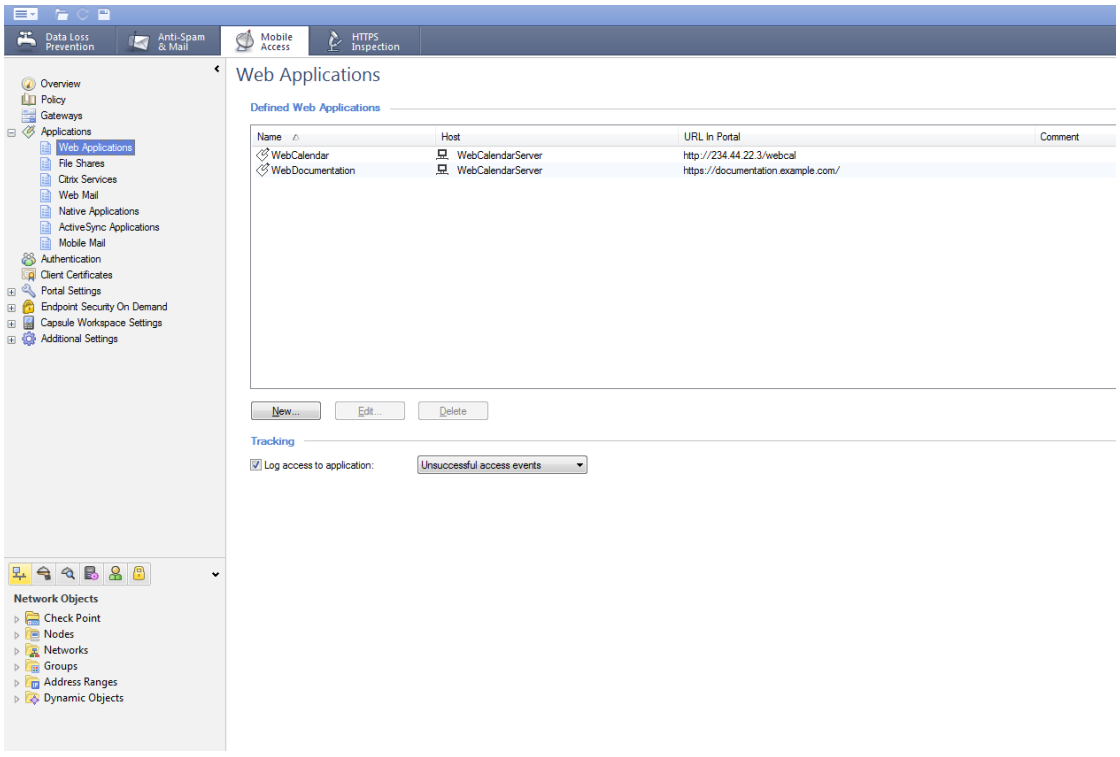
– El sistema muestra la página principal de “Mobile Access”:



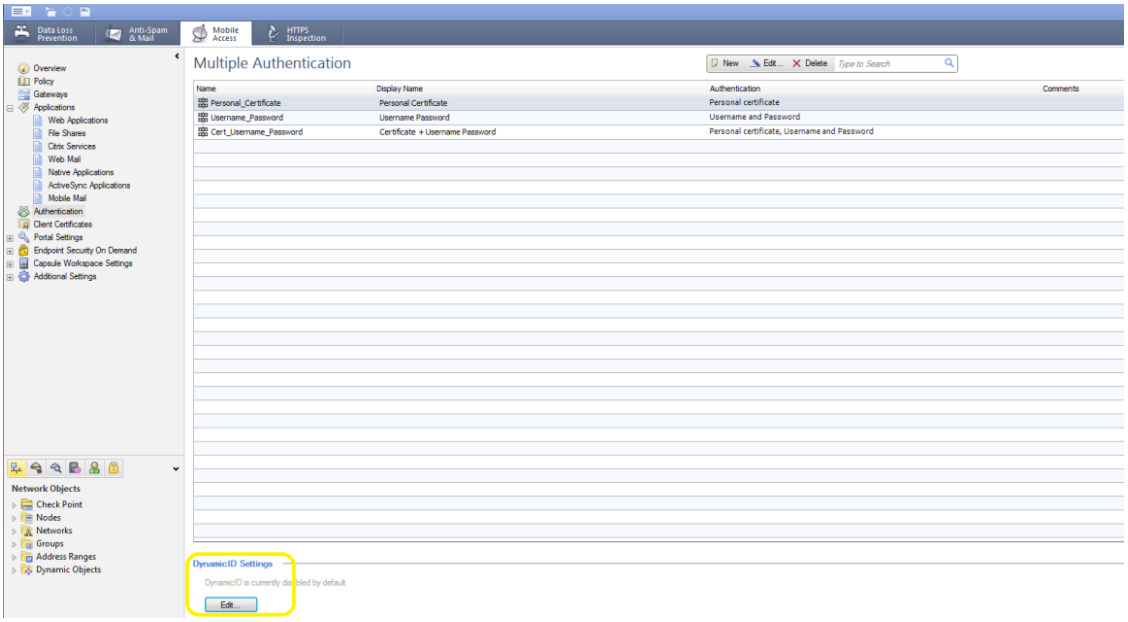
– Si se navega a la sección de políticas, se ven cuáles son las reglas asociadas a la funcionalidad de *Mobile Access* y podemos modificarlas, borrarlas y crearlas.

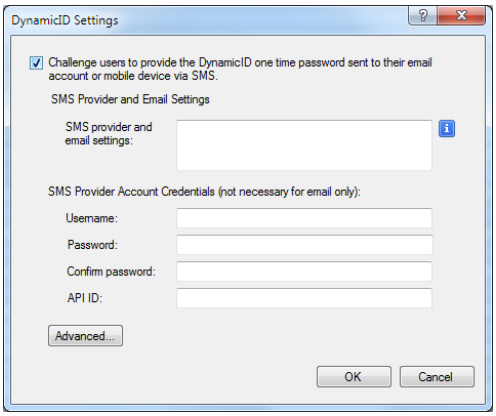


– En la sección de "Aplicaciones", existen distintos tipos de estas para poder configurarlas y hacerlas accesibles desde la VPN SSL. Entre ellas: aplicaciones web, compartición de ficheros, webmail, etc.



– Y por último en la pestaña de "Autenticación" podemos elegir, el tipo de autenticación: múltiple, autenticación (certificado y usuario+password) e incluso usar doble factor de autenticación (Dynamic ID)

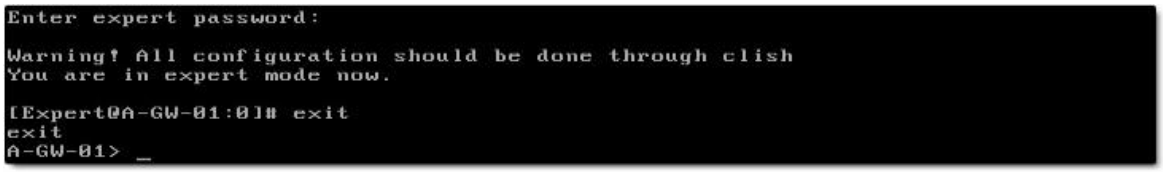

Data Loss Prevention
Anti-Spam & Mail
Mobile Access
HTTPS Inspection
Overview
Policy
Gateways
Applications
Web Applications
File Shares
Citrix Services
Web Mail
Native Applications
ActiveSync Applications
Mobile Mail
Authentication
Client Certificates
Portal Settings
Endpoint Security On Demand
Capsule Workspace Settings
Additional Settings
Multiple Authentication
New
Edit...
Delete
Type to Search
Name
Display Name
Authentication
Comments
Personal_Certificate
Personal Certificate
Personal certificate
Username_Password
Username Password
Username and Password
Cert_Username_Password
Certificate + Username Password
Personal certificate, Username and Password
Network Objects
Check Point
Nodes
Networks
Groups
Address Ranges
Dynamic Objects
DynamicID Settings
DynamicID is currently disabled by default
Edit...


DynamicID Settings
Challenge users to provide the DynamicID one time password sent to their email account or mobile device via SMS.
SMS Provider and Email Settings
SMS provider and email settings:
SMS Provider Account Credentials (not necessary for email only):
Username:
Password:
Confirm password:
API ID:
Advanced...
OK
Cancel

ANEXO A. *COMMAND LINE INTERFACE (CLI)*

Gaia utiliza una interfaz de línea de comando (CLI) fácil de usar para la ejecución de varios comandos que están estructurados con las mismas reglas sintácticas. CLI se puede usar a través de SmartConsole o un navegador web. Un sistema de ayuda mejorado y autocompletado simplifica aún más la operación del usuario.

El shell predeterminado de la CLI se llama Clish. Clish es un shell restrictivo y no proporciona acceso a funciones avanzadas de sistema y Linux. El modo experto permite el acceso avanzado del sistema y de la función de Linux al sistema, incluido el sistema de archivos. Para usar el shell experto, ejecute el comando "expert". Se debe establecer una contraseña para el modo experto antes de ejecutar el shell.



Los comandos de Gaia están organizados en grupos de comandos relacionados llamados "features".

Para ver todos los comandos que el usuario tiene permisos para ejecutar:

```
show commands
```

Para ver una lista de todas las características:

```
show commands feature <TAB>
```

Para mostrar cuánto tiempo ha estado funcionando el sistema:

```
show uptime
```

Para mostrar la información completa de la versión del sistema:

```
show version all
```

Para mostrar información sobre la versión de los componentes del sistema operativo:

```
show version os build
show version os edition
show version os kernel
```

Para mostrar el nombre del producto instalado:

```
show version product
```

ANEXO B. REFERENCIAS

- Gaia R81 Administration Guide
- Next Generation Security Gateway/Quantum Spark R81 Guide
- ClusterXL R81 (Part of Check Point Infinity) Administration Guide
- Multi-Domain Security Management R80 Administration Guide
- Threat Prevention R81 (Part of Check Point Infinity) Administration Guide
- Quality of Service R81 Administration Guide
- Data Loss Prevention R81 (Part of Check Point Infinity) Administration Guide
- Check Point R81 IPS Best Practices
- Check Point Security Management R81 Administration Guide
- Logging and Monitoring R81 Administration Guide
- Mobile Access R81 Administration Guide
- Identity Awareness R81 Administration Guide
- Site to Site VPN R81 Administration Guide
- Remote Access VPN R81 Administration Guide
- Quantum Spark 1500 1600 and 1800 Appliance Series R80.20.40 Administration Guide.
- https://downloads.checkpoint.com/fileserver/SOURCE/direct/ID/121737/FILE/CP_R80.20.40_1500_1600_1800_Appliance_Series_AdminGuide_Locally_Managed.pdf

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL