centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1302

Procedimiento de empleo seguro
McAfee Network Security Platform (NSP)

Mayo 2021

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2021.05.11 16:38:45 +02'00'

© Centro Criptológico Nacional, 2021
NIPO: 083-21-099-3.

Fecha de Edición: Mayo de 2021

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
Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1 INTRODUCCIÓN

1. ***McAfee Network Security Platform (NSP)*** es un Sistema de Detección y Prevención de Intrusiones (IDPS) de próxima generación que detecta y bloquea amenazas de *malware* sofisticadas en la red. Emplea técnicas avanzadas de detección y emulación, y va más allá de la comparación con patrones para ofrecer protección contra los ataques ocultos con un alto grado de precisión.

2. Para satisfacer las necesidades de las redes más exigentes, la plataforma puede adaptarse hasta 40 Gbits/s con un solo dispositivo y hasta 100 Gbit/s con dispositivos apilados. La integración de la solución de IPS simplifica las operaciones de seguridad mediante la combinación de la información en tiempo real de McAfee Global Threat Intelligence y los datos contextuales completos sobre usuarios, dispositivos y aplicaciones, con el fin de responder de manera rápida y precisa a los ataques que se propagan por la red.

3. El producto es una combinación de dispositivos *hardware* (*appliances*) y *software* que detecta de forma precisa y previene intrusiones, ataques de denegación de servicio (DoS), ataques de denegación de servicio distribuido (DDoS) y uso indebido de la red. El producto combina detección y prevención de intrusiones en tiempo real para ser un sistema de seguridad de la red más completo y efectivo.

4. En el siguiente esquema se puede comprobar los componentes que forman parte del producto:

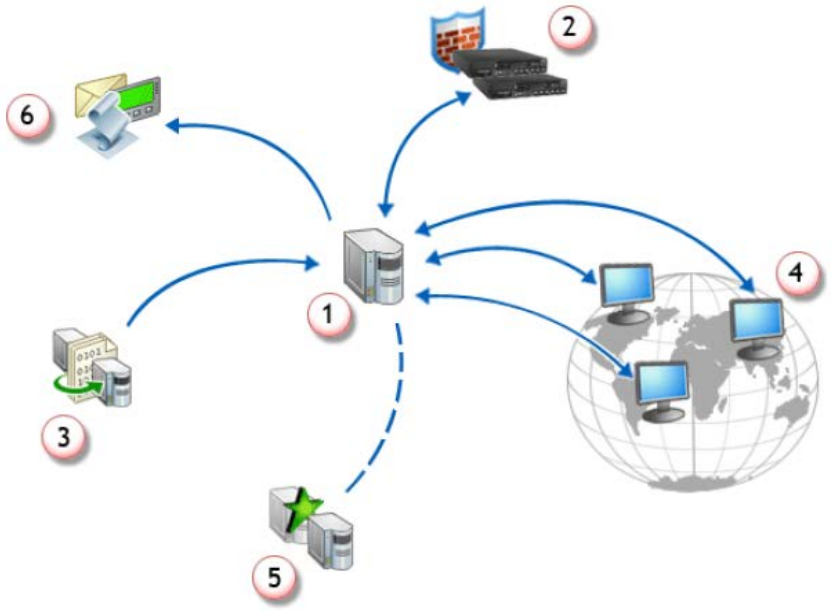

Ilustración 1. Componentes que forman el producto

5. Los componentes que se visualizan en el esquema anterior son los siguientes:

   a) **Network Security Manager (Manager).** Es una combinación de dispositivos de red y software creada para la detección y prevención precisa de intrusiones, ataques de denegación de servicio (*DoS – Denial of Service*), ataques de denegación de servicio distribuidos (*DDoS – Distributed Denia lof Service),* descarga de malware y uso indebido de la red. La plataforma de seguridad de la red proporciona una completa detección de intrusiones en la red y puede bloquear, o prevenir, los ataques en tiempo real.

   b) **Network Security Sensor (IPS Sensor).** Los sensores que utiliza el producto son dispositivos de procesamiento de contenidos de alto rendimiento, escalables y flexibles, construidos para la detección precisa y prevención de intrusiones, uso indebido, malware, ataques de denegación de servicio (DoS) y ataques de denegación de servicio distribuidos. Los sensores pueden ser dispositivos físicos o virtuales. Los sensores están diseñados específicamente para manejar el tráfico a velocidad de cable, inspeccionar eficazmente y detectar intrusiones con un alto grado de precisión, y son lo suficientemente flexibles como para adaptarse a las necesidades de seguridad de cualquier entorno empresarial. Cuando es desplegado en los puntos de acceso de una red, los sensores proporcionan una monitorización en tiempo real del tráfico que transcurre por ellos para detectar actividad maliciosa y responder a la actividad maliciosa de acuerdo con la configuración realizada por el administrador.

   c) ***McAfee Update Server*.** Para que el producto detecte y proteja adecuadamente contra amenazas y actividad maliciosa, tanto el *Manager* como el *IPS Sensor* deben de ser actualizados frecuentemente con las últimas firmas y parches de *software* disponibles. Las nuevas firmas y parches de seguridad se ponen a disposición de los clientes a través del componente *McAfee Update Server*. Este servidor de actualizaciones proporciona de forma segura actualizaciones de firmas totalmente automatizadas y en tiempo real sin requerir intervención manual. La comunicación entre los componentes Manager y *Update Server* es segura mediante el uso comunicación SSL (TLS1.2).

   d) **Acceso de clientes web al *Manager* Server.** El componente *Manager* dispone de una interfaz gráfica que permite llevar a cabo cambios en su configuración a un administrador. Con carácter adicional, es posible hacer uso de un *Manager Client,* una aplicación web Java, que proporciona una interfaz de usuario basada en la web para una gestión centralizada y remota. El servidor aloja el *software* de gestión y la base de datos de gestión, sobre un sistema

operativo. A través de su interfaz gráfica es posible llevar a cabo la configuración del producto. La base de datos es de tipo relacional (RDBMS, *Relational DataBase Management System*) para almacenar información persistente sobre la configuración y los eventos. La base de datos compatible es MariaDB 10.3.13. Esta base de datos puede ser modificada a través de la configuración de la interfaz de usuario del componente *Manage*.

e) ***Manager Disaster Recovery (MDR) server*.** Este componente permite restablecer la configuración de los componentes *Manager* y de los sensores, los datos archivados y las políticas configuradas. Para ello, es necesario disponer de dos (2) componentes *Manager* desplegados. El *Manager secundario* se mantiene en un estado latente por defecto y se encarga de monitorizar el estado de salud del *Manager principal* y de realizar una copia de la información de configuración periódicamente. Los sensores conectados mantienen una comunicación constante con ambos componentes, enviando mensajes de alertas y registros de auditoría. En caso de que uno de los componentes *Manager* sufra un fallo que le impida continuar con su funcionamiento durante un tiempo y vuelva a entrar en funcionamiento una vez solventado el fallo, este se actualizará con las alertas perdidas y los datos de los registros de auditoría generados durante el fallo mediante el proceso de sincronización establecido con el *Manager compañero.* Esta sincronización restaura las alertas perdidas y los datos del registro de las 24 horas anteriores (restaurando como máximo 10000 registros).

f) Notificación de alertas, email, generación de scripts.

6. La función principal del dispositivo es la de analizar tráfico de un segmento de red seleccionado y responder cuando un ataque es detectado. El dispositivo examina la cabecera y la porción de datos de cada paquete de red, realizando una búsqueda de patrones y comportamiento en el tráfico de red e indicando actividad maliciosa. Los marcará de acuerdo con las políticas definidas. Estas políticas determinan qué tipo de ataques se deben detectar y cómo responder mediante el uso de contramedidas.

7. Si un ataque es detectado, un sensor IPS físico o virtual responderá de acuerdo a su política configurada. Un sensor puede realizar diversos tipos de respuesta a ataques, incluyendo generación de alertas y logs sobre los paquetes, reseteando las conexiones TCP, depurando paquetes maliciosos e incluso bloqueando paquetes de ataque previamente a que alcancen su objetivo.

8. Adicionalmente a su función principal de prevenir ataques, reconocimiento y ataques de denegación de servicio, un sensor también es capaz de realizar lo siguiente:

a) **Detección de *malware*.** Un sensor utiliza varios métodos para inspeccionar los ficheros que se están descargando en busca de *malware* embebido. Si se detecta *malware*, el sensor bloquea la descarga y tomará acciones de respuesta adicionales.

b) **Hacer cumplir reglas de acceso al cortafuegos.** Es posible definir reglas de acceso al cortafuegos (similar a ACLs, *Access Control Lists*) en el componente *Manager*. Posteriormente, se puede configurar un sensor para forzar el cumplimiento de las reglas creadas en una red determinada.

c) **Proporcionar y facilitar calidad de servicio (QoS).** Es posible configurar un sensor físico para proporcionar calidad de servicio utilizando la técnica de tasa limitada. Adicionalmente, un sensor físico puede facilitar servicios diferenciados y IEEE 802.1p diferenciando tráfico y marcándolo adecuadamente.

d) **Proporcionar conexión limitada de servicios.** En función de la configuración, un sensor puede limitar el número de conexiones que un equipo determinado puede establecer. Una de las ventajas de la limitación de conexión consiste en la posibilidad de minimizar los ataques de denegación de conexión (DoS) basados en conexión.

e) **Exportar datos NetFlow.** Si se despliega el componente *McAfee Network Threat Behavior Analysis (NTBA),* es posible configurar un sensor para exportar datos *NetFlow* al *appliance* NTBA.

9. El componente *Manager Server* aloja el *software* de gestión y la base de datos de gestión. Es un servidor ejecutado en un sistema operativo. Es posible acceder de forma remota haciendo uso de un navegador web. A través de su interfaz gráfica es posible llevar a cabo la configuración del producto. La base de datos es de tipo relacional (RDBMS, *Relational DataBase Management System*) para almacenar información persistente sobre la configuración y los eventos. La base de datos compatible es MariaDB 10.3.13. Esta base de datos puede ser modificada a través de la configuración de la interfaz de usuario del componente *Manage*.

2 OBJETO Y ALCANCE

10. La configuración evaluada del producto y por lo tanto incluida en la presente guía de empleo seguro consiste en un *software* instalado en un *appliance* y uno o más sensores. Las versiones de cada uno son las siguientes:

    a) NSM Linux *appliance* 9.1.21.20.

    b) NS Sensor *appliances* 9.1.17.100.

11. El producto ha sido cualificado para la familia "Dispositivos de prevención y detección de intrusiones", incluida en la categoría "Monitorización de la Seguridad" del Catálogo de Productos y Servicios STIC (CPSTIC).

3 ORGANIZACIÓN DEL DOCUMENTO

12. El presente documento se estructura en las secciones indicadas a continuación:

    a) **Apartado 4**. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de despliegue e instalación del producto.

    b) **Apartado 5.** En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

    c) **Apartado 6.** En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

    d) **Apartado 7.** En este apartado se incluye una lista de tareas a revisar para verificar que se han llevado a cabo cada una de las recomendaciones y configuraciones descritas en la presente guía de empleo seguro.

4 FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

13. El procedimiento de recepción segura del producto, al tratarse de una combinación *hardware/software* está formada por dos (2) procesos:

    a) Entrega del componente hardware (appliance). Hay que tener en consideración los siguientes pasos:

        i. Cuando se recibe el dispositivo, se recomienda inspeccionar el paquete y el dispositivo en buscar de signos de daños o manipulación, incluida la cinta de embalar que protege el contenedor de envío, donde los signos de manipulación serían evidentes. Si existe algún signo de daños, manipulación incorrecta o alteración, es necesario ponerse en contacto con el Soporte de McAfee con carácter inmediato a fin de recibir instrucciones. Se recomienda dada esta situación, que no se realice la instalación del producto.

        ii. Verificar que el paquete contenga todos los elementos indicados en el albarán.

        iii. Si se va a llevar a cabo una instalación FIPS, es preciso localizar el sello a prueba de manipulación dentro del paquete de accesorios incluido en el contenedor de envío.

    b) Entrega del componente software. Al igual que sucede con todos los productos de McAfee, es necesario llevar a cabo los siguientes pasos:

        i. Una vez adquirido el producto, su recepción consiste en un correo electrónico que incluye los siguientes datos:

            – *Account Number*

            – *Grant Number*

            – *Purchase order Number*

        ii. Estos datos proporcionan un inicio de sesión al portal de descargas oficial (cuya URL será proporcionada en el mismo correo electrónico) donde será necesario introducir el correo electrónico utilizado para la adquisición del producto, así como el *Grant Number* del mismo. Una vez se consigue el acceso al servidor de descargas, se podrán ver los productos disponibles para descargar en la sección *Products* de la página *My Products.* De este modo se puede proceder a la descarga

del producto y de sus distintos componentes. Si se necesita una copia de la licencia, se puede obtener de la sección *License Keys.*

iii. El producto se encuentra firmado digitalmente mediante un certificado de McAfee. Para verificar que los distintos ficheros descargados han sido firmados correctamente, el usuario puede extraer los ficheros incluidos dentro de los ficheros comprimidos y comprobar, haciendo clic derecho en el fichero y, haciendo clic en la opción *Propiedades,* seleccionar la sección *Digital Signature.* En el campo de *Signer Information* se podrá verificar la procedencia de dicho certificado. Además, en cada descarga, se incluye un valor *hash* haciendo uso de SHA-256, lo cual permite llevar a cabo una descarga segura, manteniendo la integridad de la misma. De este modo, se puede dar por concluido el proceso de obtención del producto y de sus componentes.

4.2 ENTORNO DE INSTALACIÓN SEGURO

14. Los componentes del producto deben instalarse en un entorno en el que el personal técnico encargado dispone de autorización para la configuración, despliegue y mantenimiento del producto.

4.3 REGISTRO Y LICENCIAS

15. Para realizar el registro de la licencia del producto hay que obtener la clave de registro del producto en el servidor de descarga *McAfee Download Server*. Si se ha saltado el proceso de registro de producto durante el inicio de sesión inicial después de la instalación o actualización, ir a *Manager* → *<Admin Domain Name>* → *Summary (Manager* → *Summary),* y hacer clic en *Register Product* y seguir los pasos del 3 en adelante de la lista descrita a continuación:

    a) Iniciar sesión en el componente Manager.

    b) Leer y aceptar el acuerdo de licencia haciendo clic en Activate.

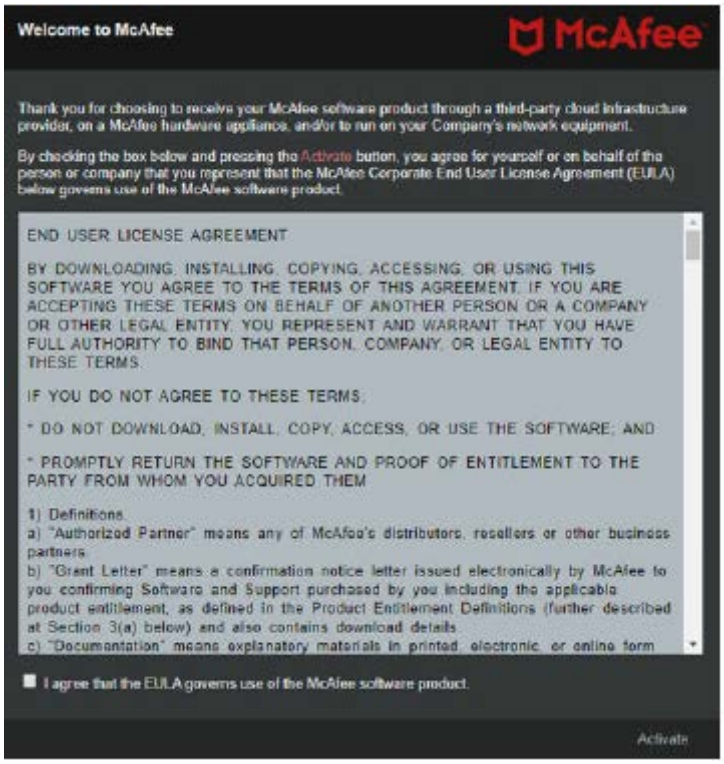

Ilustración 2. Acuerdo de licencia del producto

c) Aparecerá el diálogo *Product Registration*. En el caso de que no se disponga de una clave de registro disponible hacer clic en *"Lost Key?"* para acceder al proceso de recuperación de la clave de registro.

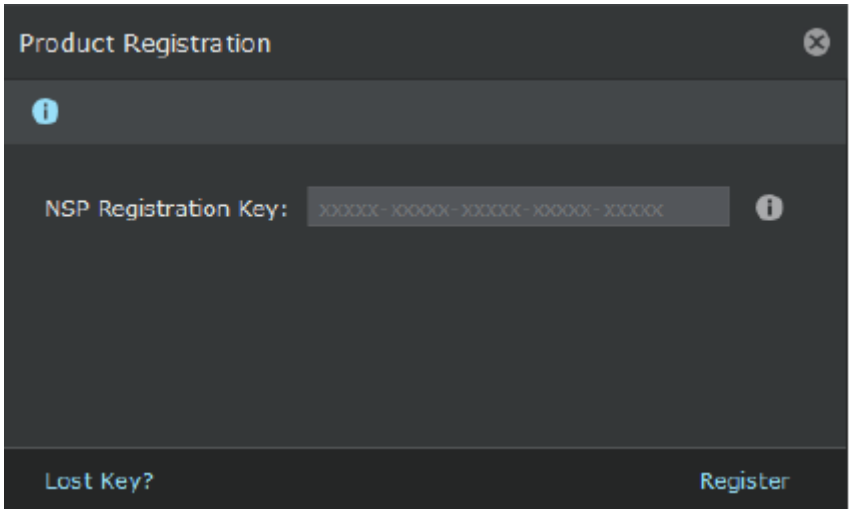

Ilustración 3. Diálogo para introducir la clave del producto

d) Introducir la clave de registro del producto y hacer clic en Register.

e) Una vez que el proceso de registro del producto esté completado, un diálogo de información aparece con un mensaje de registro realizado correctamente.

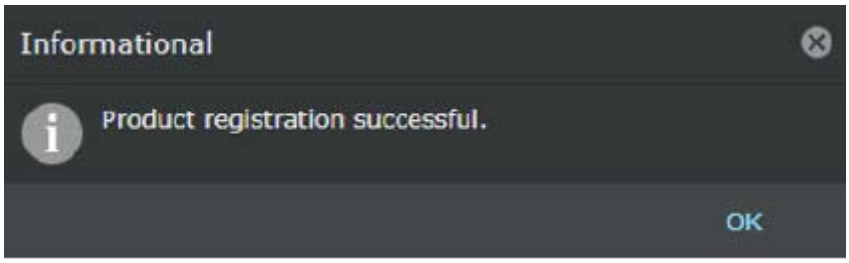

Ilustración 4. Ventana que informa de que el producto se ha instalado correctamente.

4.4 CONSIDERACIONES PREVIAS

16. Antes de llevar a cabo la instalación, es necesario asegurarse de completar las siguientes tareas:

    a) El servidor, donde el componente software Manager será instalado, debe de estar configurado y listo.

    b) Se debe de disponer de privilegios de administrador para el servidor que aloje el componente Manager.

    c) Este servidor debe de ser dedicado, hardenizado, y situado en su propia subred. Este servidor no debe de ser utilizado para el uso de programas de mensajería instantánea u otras funciones no seguras en Internet.

    d) Asegurarse de que se cumplen los requisitos hardware o al menos, los requisitos mínimos.

    e) Asegurarse que se ha asignado una dirección IP estática en el servidor *Manager*.

    f) Si es necesario, configurar la resolución de nombres para el *Manager*.

    g) Disponer del fichero de licencia requerido y el *Grant Number*. Es necesario tener en cuenta que no es necesario un fichero de licencia para utilizar la versión 6.0.7.5 o superior del Manager/Central Manager.

    h) Acumular el número requerido de cables y (admitidos) GBIC, SFP o XFP. Asegurarse que el hardware sea aprobado por McAfee o un proveedor de apoyo. Asegurar que el número requerido de adaptadores *Network Security Platform*, enviados junto con los sensores, están disponibles.

    i) Se necesitarán cables cruzados para los puertos de monitorización 10/100 o 10/100/1000 si se conectan directamente a un cortafuegos o a un router, o nodo final. De lo contrario, se requieren cables de conexión estándar para los puertos de Fast Ethernet.

j) Si corresponde, identificar los puertos que se van a reflejar, y el técnico con el conocimiento y los derechos suficientes para hacerlo.

k) Asignar las direcciones IP estáticas adecuadas para el sensor. Para los sensores, no puede asignarse direcciones IPs utilizando DHCP.

l) Identificar los hosts que pueden causar falsos positivos, por ejemplo, servidores de caché HTTP, servidores DNS, retransmisores de correo, administradores SNMP y los escáneres de vulnerabilidad.

17. De forma adicional, es necesario tener en cuenta los siguientes requisitos funcionales:

a) Instalar *Wireshark* (antes conocido como *Ethereal* http://www.wireshark.com) en los equipos PC cliente. *Ethereal* es un protocolo de red analizador para servidores Unix y Windows, utilizado para analizar los registros de paquetes creados por los sensores.

b) Asegurarse de que está instalada la versión correcta de JRE en el sistema cliente. Esto puede ahorrar mucho tiempo durante el despliegue. Durante el primer inicio de sesión del componente Manager, se mostrará una ventana en la que se podrá descargar e instalar la versión apropiada del *software* JRE.

c) El servidor *Manager* utiliza el puerto 4167 como puerto de origen UDP para enlazar para IPv4 y el puerto 4166 para IPv6. Si se disponen de sensores desplegados detrás de un cortafuegos, es necesario actualizar sus reglas de forma que los puertos 4167 y 4166 estén abiertos para que el canal de comando SNMP funcione entre esos sensores y el administrador. Esto es también aplicable a un cortafuegos local que se ejecuta en el servidor *Manager*.

d) Determinar un modo de sincronizar el componente *Manager* con una hora correcta. Para evitar desvíos temporales, por ejemplo, hay que configurar el componente Manager a un servidor de tiempo NTP. Si se cambia la hora en el servidor Manager, se perderá la conectividad con todos los sensores y el *McAfee Network Security Update Server* porque el protocolo SSL es sensible al tiempo.

e) Si se configura la funcionalidad *Manager Disaster Recovery (MDR),* es necesario asegurarse de que la diferencia de tiempo entre los nodos primarios y los secundarios es menor a 60 segundos (si la diferencia entre ambos supera los dos minutos, la comunicación de los sensores se perderá).

f) Si se necesita una nueva instalación del componente *Manager* en una máquina donde ya se encuentra instalado, es necesario asegurarse de que el

este ha sido desinstalado y los respectivos directorios son eliminados antes de realizar la nueva instalación.

18. Es recomendable el uso de un cortafuegos de escritorio para el servidor de *Manager*. Ciertos puertos son utilizados por los componentes de *McAfee Network Security Platform*. Algunos de estos son necesarios para la comunicación cliente-servidor de *Manager* y los sensores. **Todos los puertos restantes innecesarios deben de ser deshabilitados.**

19. McAfee recomienda configurar un cortafuegos de filtrado de paquetes para bloquear las conexiones a los puertos 8551, 8552, 3306, 8007, 8009, y 8552 del servidor **Manager.** El objetivo es denegar las conexiones a estos puertos si las conexiones no son iniciadas por el anfitrión local. Las únicas conexiones que deberían permitirse son los del propio servidor *Manager*, es decir, *localhost*. Por ejemplo, si otra máquina intenta conectarse al puerto 8551, 8552, 3306, 8007 y 8009 el cortafuegos debería bloquear automáticamente cualquier paquete enviado.

20. Si el cortafuegos se sitúa entre el *Sensor*, *Manager* o un cliente administrativo, el cual incluye un cortafuegos local en el componente *Manager*, deben de abrirse los siguientes puertos:

    a) 4167 y 4166 UDP – Protocolo SNMPv3 por defecto.

    b) 8500 UDP – Protocolo SNMPv3 por defecto.

    c) 8501 TCP – Propietario (instalación de canal utilizando un certificado SHA-256 de 2048 bits).

    d) 8502 TCP – Propietario (alerta de canal/canal de control utilizando un certificado SHA-256 de 2048 bits).

    e) 8503 TCP – Propietario (canal de registro de paquetes usando el certificado SHA-256 de 2048 bits).

    f) 8504 TCP – Propietario (canal de transferencia de ficheros)

    g) 8506 TCP – Propietario (canal de instalación para los certificados SHA-1 de 2048 bits).

    h) 8507 TCP – Propietario (canal de alerta/canal de control usando el certificado SHA-1 de 2048 bits).

    i) 8508 TCP – Propietario (canal de registro de paquetes usando el certificado SHA-1 de 2048 bits).

    j) 8509 TCP – Propietario (canal de transferencia de archivos masiva utilizando certificados SHA-1 de 2048 bits).

k) 8510 TCP – Propietario (canal de transferencia de archivos masiva utilizando certificados SHA-256 de 2048 bits).

l) 443 TCP – Protocolo HTTPS.

m) 80 TCP – Interfaz de usuario web.

n) 8005 TCP – Utilizado por el *Manager* para recibir instrucciones de apagado.

o) 22 TCP – Protocolo SSH.

p) 3306 TCP – Utilizado internamente para conectar *MariaDB* con el *Manager*.

q) Puertos 8500 al 8510 están alojados por el *Manager*.

21. En los apartados *g), h)* y *j)* se hace mención al uso del algoritmo SHA-1. La utilización de certificados **SHA-1** para los puertos mencionados se debe a que dichos puertos tienen la función de **proporcionar compatibilidad entre versiones antiguas del producto**. Por lo tanto, para el **caso de una instalación nueva** en un entorno **donde no coexistan versiones anteriores**, dichos puertos no se utilizarán y el producto **solamente** utilizara el algoritmo **SHA-256** para sus certificados.

22. El propio fabricante incluye en su guía de instalación [REF5] la sección *'Migration from SHA1 to SHA256 signing algorithm*'. En esta sección se listan una serie de pasos para llevar a cabo la actualización del producto de forma que se utilice SHA-256 para el caso en que sea necesaria llevar a cabo la migración desde una versión más antigua. Estos pasos se resumen a continuación:

    a) En primer lugar, se debe actualizar la versión del *Manager* para que soporte claves RSA de 2048-bits con *sha256WithRSAEncryption*.

        i. Usar *'setup.bin.usigned'* para actualizar versiones *9.1.7.49, 9.1.7.63* y *9.1.7.73*.

        ii. Usar *'setup.bin'* para actualizar las versiones *9.1.7.75 y 9.1.7.77*.

    b) Por último, actualizar el software de los sensores para que sea posible realizar la migración de los puertos. Si no se realiza esta operación, el Manager se detendrá y lanzará el error *'Unsupported Device Certificate Strength Detected'.*

23. Algunas operaciones del componente *Manager* pueden entrar en conflicto con los procesos de análisis de *McAfee VirusScan* o de cualquier otro *software* antivirus que se ejecute en el componente *Manager*. Por ejemplo, el *software* antivirus podría analizar todos los archivos temporales creados en el directorio de instalación del componente Manager, lo que podría ralentizar su rendimiento. Por lo tanto, es necesario asegurarse de excluir el directorio de instalación del

Manager y sus subdirectorios de los procesos de análisis antivirus. Específicamente, hay que asegurarse de excluir las siguientes carpetas:

a) Directorio de instalación de *Manager**MariaDB* y sus subdirectorios. Si no se excluyen los directorios, las capturas del producto pueden resultar en el borrado de ficheros esenciales de MariaDB.

b) Directorio de instalación de *Manager**App**temp**tftpin**malware*\ y sus subdirectorios.

24. McAfee *VirusScan* incluye una opción (habilitada por defecto) para bloquear todas las conexiones salientes sobre el puerto TCP 25. Esto ayuda a reducir el riesgo de propagación de un gusano en un equipo mediante el uso del protocolo SMTP. *VirusScan* evita bloquear las conexiones SMTP salientes de clientes de correo legítimos, como Outlook y Eudora, al incluir procesos utilizados por esos productos en una lista de exclusión. En otras palabras, *VirusScan* se envía con una lista de procesos que permitirá crear conexiones de salida del puerto TCP 25; a todos los demás procesos se les niega ese acceso.

25. El componente Manager aprovecha la API de *JavaMail* para enviar notificaciones SMTP. Si se habilita la notificación SMTP y también se ejecuta VirusScan 8.0i o superior, se debe añadir *java.exe* a la lista de procesos excluidos. Si no se crea explícitamente la exclusión dentro de VirusScan, se observará un error de *Mailer Unreachable* en el estado operativo del *Manager* cada vez que se intente conectar a su servidor de correo configurado. Para añadir la exclusión, es necesario seguir los siguientes pasos:

    a) Ejecutar la consola de *VirusScan*.

    b) Clic derecho en la tarea llamada *Access Protection* y elegir *Properties*.

    c) Marcar la regla llamada *Prevent mass mailing worms from sending mail*.

    d) Hacer clic en Edit.

    e) Añadir el fichero java.exe a la lista de *Processes to Exclude*.

    f) Clic OK para guardar los cambios.

26. En el caso de que el producto sea utilizado junto a *McAfee Endpoint Security* puede ocurrir un error durante el proceso de escaneo *On-Access Scan* de esta herramienta. El error puede impedir la copia de seguridad. Para solucionarlo, se necesita excluir el directorio del producto de *On-Access Scan*. Para ello, es necesario seguir los siguientes pasos:

    a) Desde el menú de inicio del servidor donde se encuentra instalado el componente Manager abrir *McAfee Endpoint Security*.

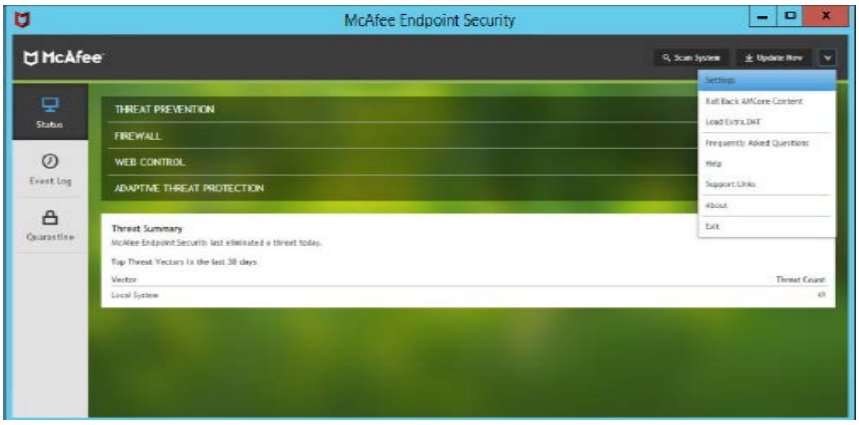

Ilustración 5. Interfaz de McAfee Endpoint Security

b) Hacer clic en *Settings*.

c) Clic en *Threat Prevention* → *Show Advanced* → *On-Access Scan*

Ilustración 6. Panel Threat Prevention

d) En la sección *Process Setting*, seleccionar la sección Standard bajo el tipo de proceso.

e) Clic en *Add* en la sección *Exclusions*.

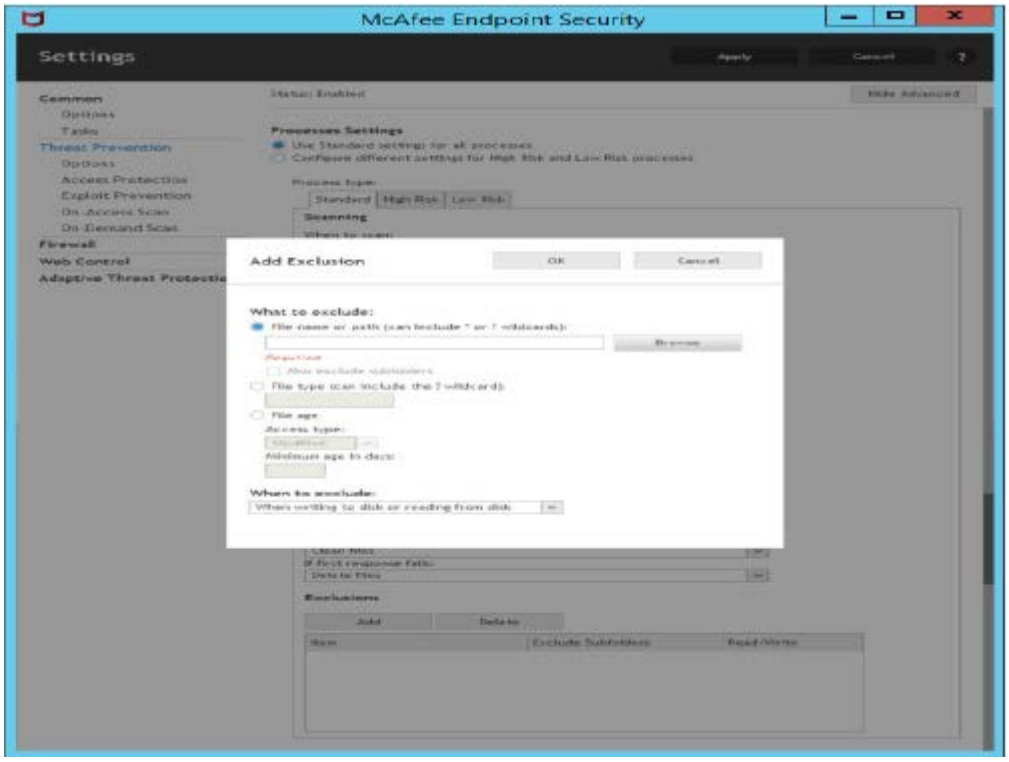

Ilustración 7. Ventana Emergente donde añadir exclusiones

f) En la página de *Add Exclusions*, clic en *Browse*.

g) Seleccionar el directorio *Network Security Manager*.

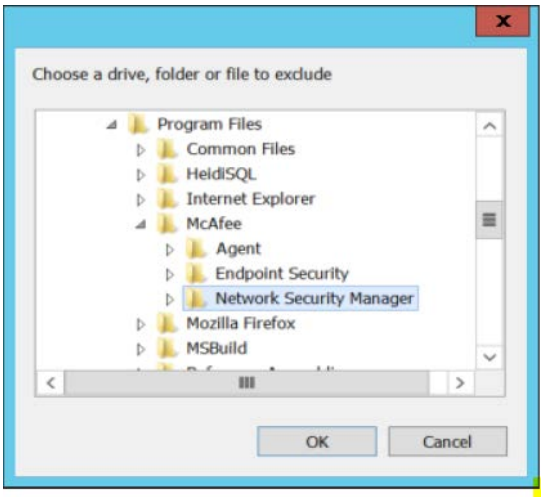

Ilustración 8. Ventana de selección del directorio

h) Seleccionar *'Auto exclude subfolders'*. Clic en OK.

i) Para los tipos de procesos *High Risk* y *Low Risk*, repetir los pasos 5 a 8.

j) Clic en *Apply*.

27. Del mismo modo, en algunos escenarios, durante el proceso de *On-Demand Scan* con el uso de la herramienta *McAfee Endpoint Security* también impide realizar una copia de seguridad de la base de datos del componente *Manager*. En estos casos es necesario excluir, del mismo modo, el directorio del producto *Network Security Manager* desde la opción *On-Demand Scan.*

28. Hay que tener en cuenta que estos errores que aquí se muestran suceden al utilizar el producto junto con *McAfee Endpoint Security*, el cual es independiente al producto objeto del presente procedimiento de empleo seguro.

4.5 INSTALACIÓN

29. El producto es un *appliance* que precisa de la instalación de un sistema operativo sobre el cual se puede ejecutar el *software* denominado como *Manager*. La instalación puede realizarse en el sistema operativo *Windows Server* o en el sistema operativo propietario de McAfee basado en Linux, **McAfee Linux Operating System (MLOS)**.

30. **MLOS es el sistema operativo cubierto en la cualificación y por la presente guía de empleo seguro**. La imagen para servidores ESXi crea una instancia virtual del componente Network Security Manager ejecutado en MLOS. Es posible crear una instancia del componente Manager haciendo uso de una imagen OVA, teniendo en cuenta las siguientes consideraciones:

    a) Es necesario tener una red virtual de origen y destino definida en el servidor ESXi.

    b) Es necesario disponer de más de 300GB de espacio disponible en el servidor ESXi ya que la imagen está creada con la capacidad mencionada.

31. Para realizar la instalación, es necesario llevar a cabo los siguientes pasos:

    a) En el cliente *VMware vSphere*, seleccionar *File → Deploy OVF Template.*

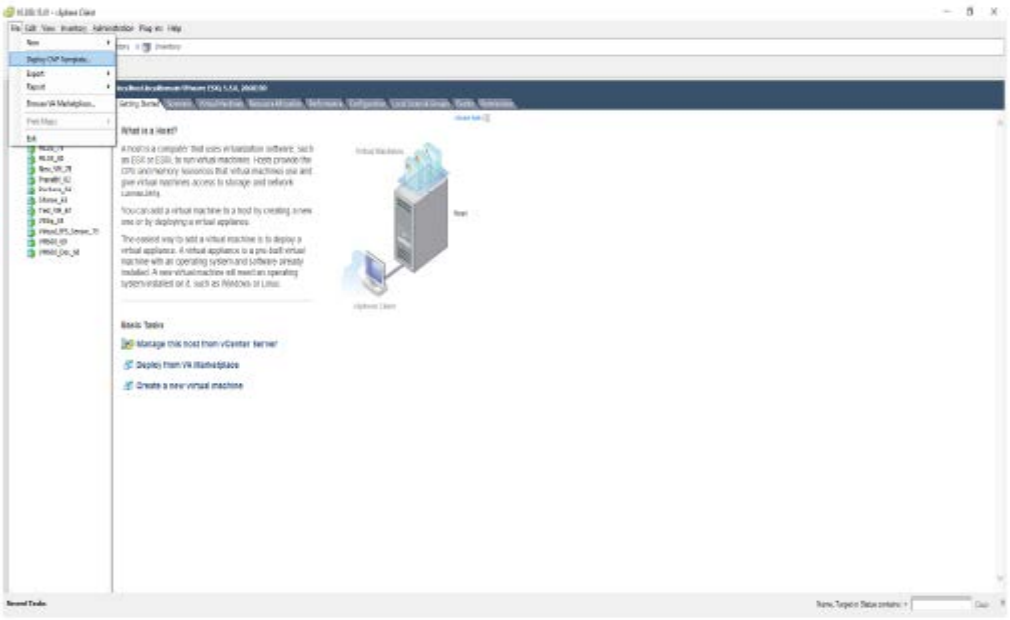

Ilustración 9. Interfaz del cliente VMware vSphere

b) En la sección *Source*, clic en *Browse* y navegar a la localización donde la imagen OVA está situada y seleccionar el fichero Manager OVA.

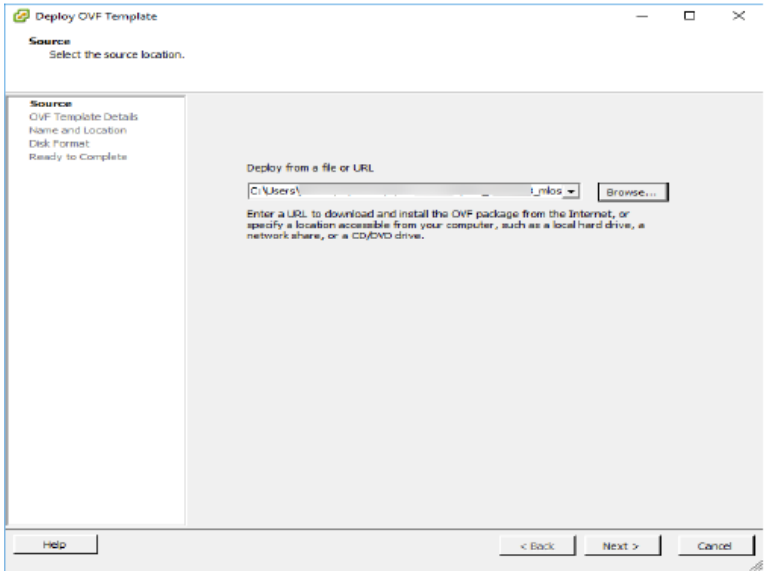

Ilustración 10. Carga de OVA

c) Clic en *Next*. Se abrirá la sección *OVF Template Details*.

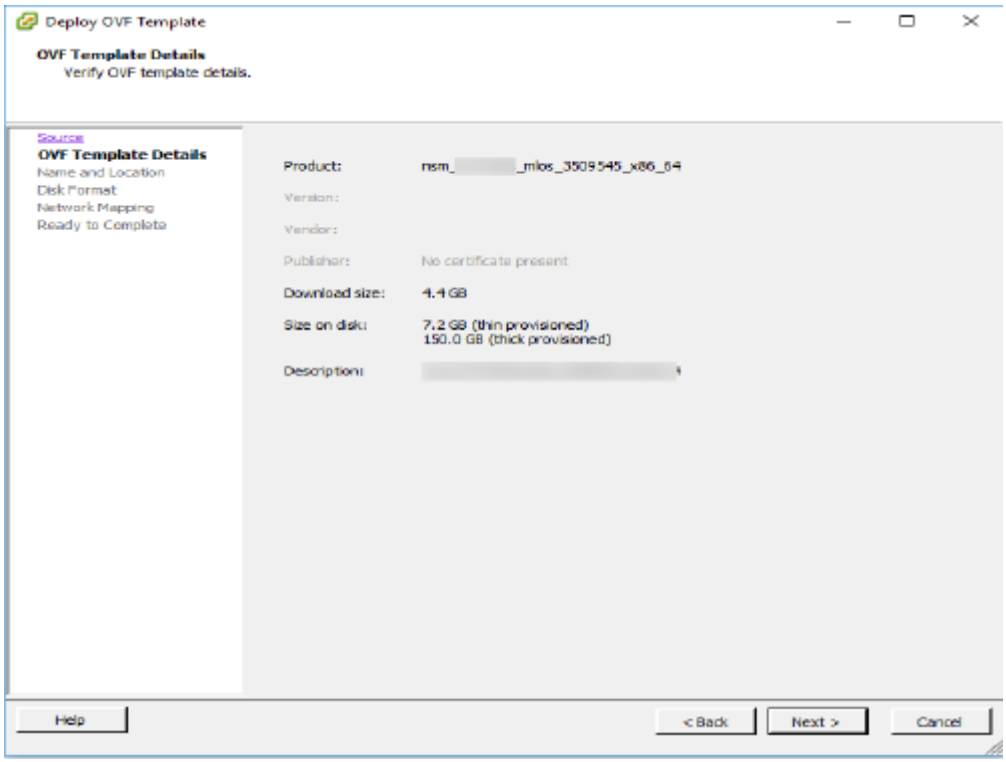

Ilustración 11. Detalles de la plantilla

d) Clic en *Next*. La sección *Name* and *Location* se abre.

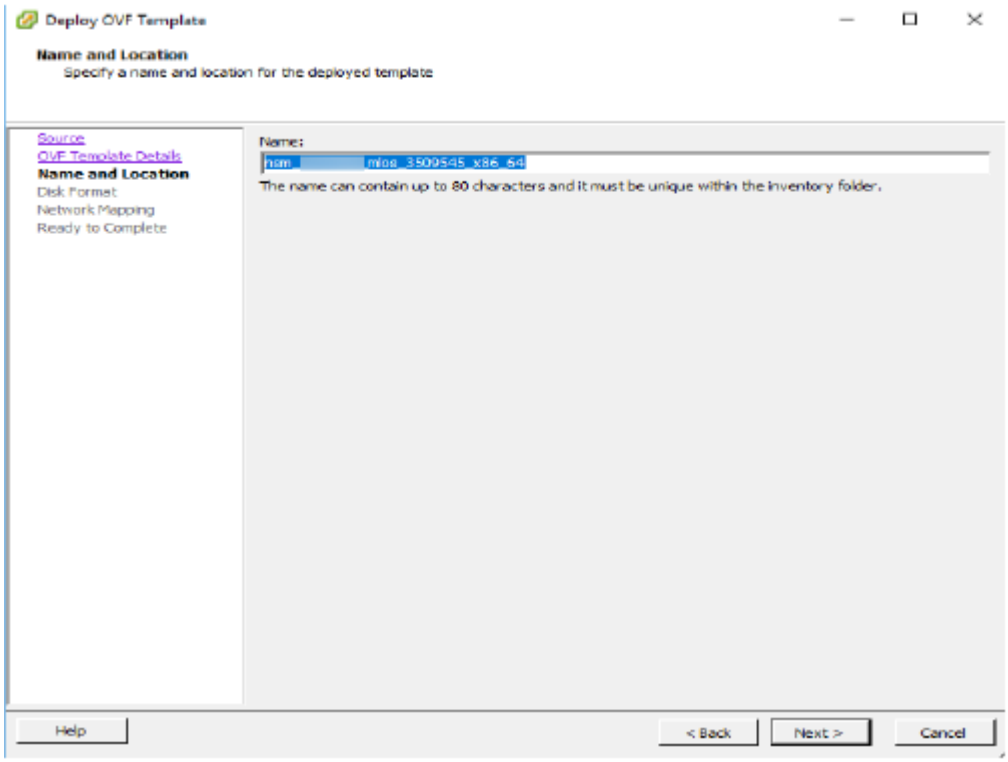

Ilustración 12. Campo de nombre y ruta

e) Por defecto, se muestra el nombre del fichero OVA. Opcionalmente es posible introducir un nombre para el componente Manager en el campo *Name*. En este ejemplo, el componente Manager se denomina *My_Company*. El nombre puede contener hasta 80 caracteres incluyendo números y caracteres especiales.

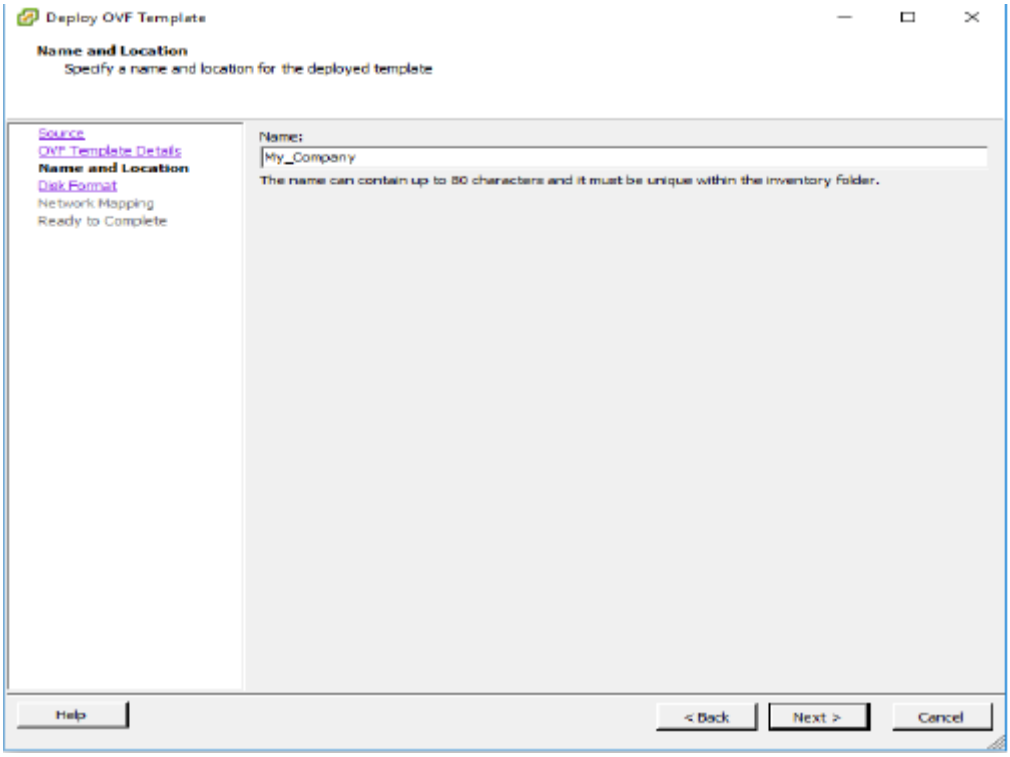

Ilustración 13. Nombre del componente Manager en el ejemplo

f) Clic en *Next*. La sección *Disk Format* se abre.

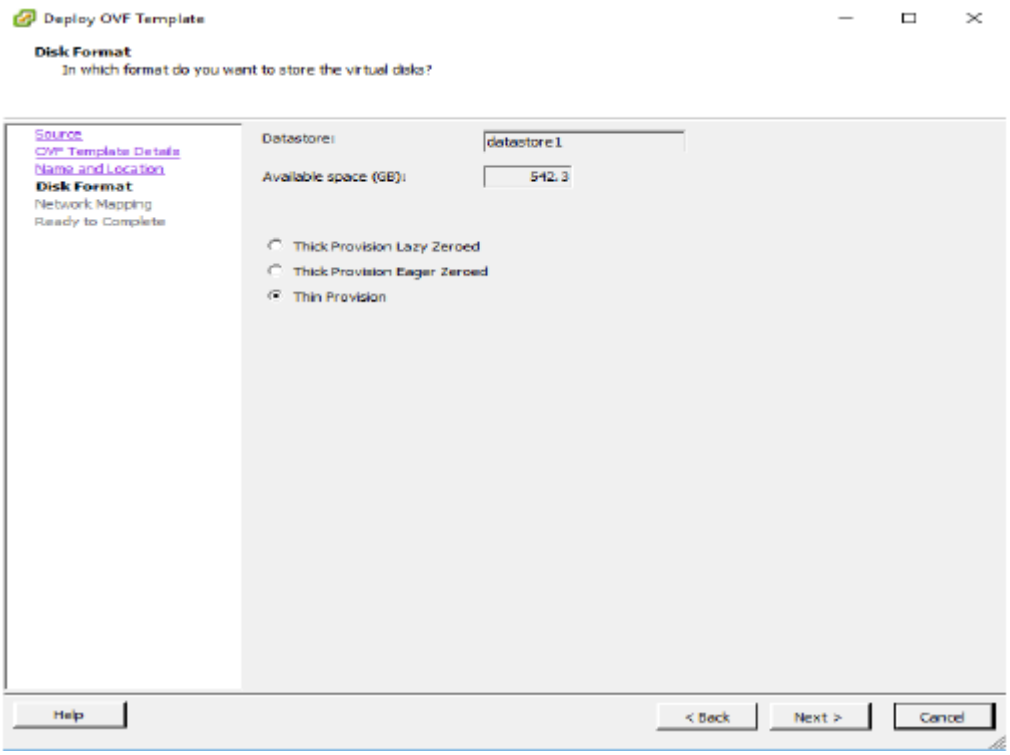

Ilustración 14. Campo Disk Format

g) Seleccionar el formato de aprovisionamiento de disco (*thick* o *thin*), dependiendo de la cantidad de espacio físico de almacenamiento disponible. McAfee recomienda la opción por defecto, es decir, el aprovisionamiento *thin*. Clic *Next*.

h) En la sección *Network Mapping*, es necesario realizar un mapeo de las redes de origen y destino para el Manager para los puertos de red preconfigurados en el servidor ESXi.

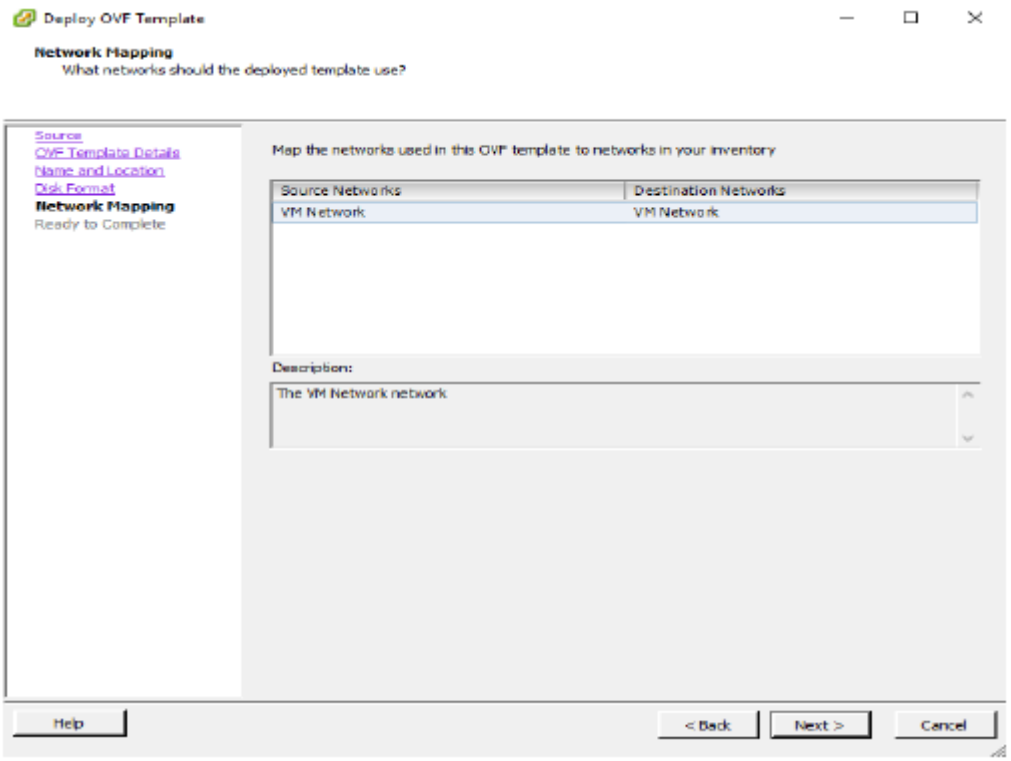

Ilustración 15. Campo Network Mapping

i) Clic *Next*. Se abrirá la sección *Ready to Complete*.

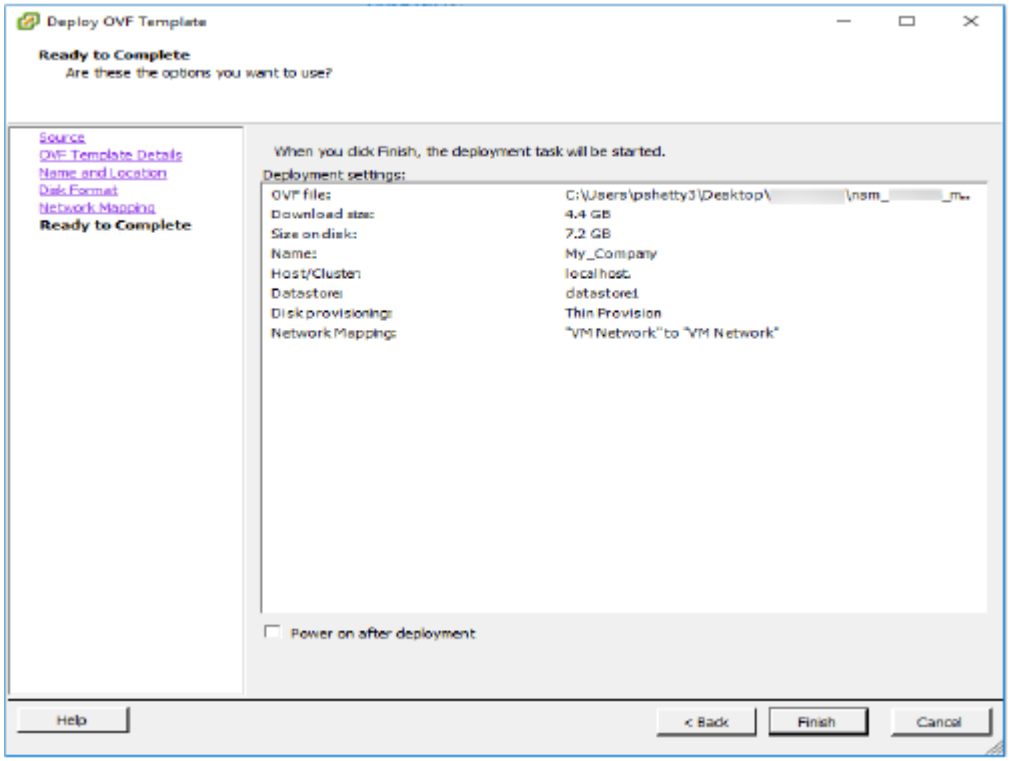

Ilustración 16. Campo de verificación de características

j) Verificar la configuración y seleccionar *Power on after deployment*.

k) Clic en *Finish* para desplegar la máquina virtual Linux con el componente *Manager*.

l) Una vez que el despliegue está completo, se puede configurar el componente *Manager* haciendo uso de SSH.

32. Adicionalmente, es necesario llevar a cabo el despliegue de los dispositivos sensores. Se puede acceder a la página *Devices* desde la barra de menú del componente *Manager*. Esta página permite gestionar el grupo de la red de sensores de seguridad integrados con el componente Manager. Los ajustes de configuración para un dominio específico en la pestaña *Global* establecen las reglas generales que se aplican por defecto a todos los dispositivos físicos añadidos dentro del componente *Manager*. Estos dispositivos aparecen en la lista de dispositivos visitables en el desplegable de dispositivos y adoptan las reglas generales de los dominios parentales.

33. El proceso de añadir y configurar un sensor implica invocar al asistente de instalación del sensor, importar conjuntos de firmas de un directorio local, agregar un sensor al *Manager*, asignar la configuración del puerto de un sensor, actualizar la configuración del sensor, seleccionar el método de actualización del juego de firmas, descargar el último juego de firmas, configurar el sensor mediante la línea de comandos, aplicar políticas a las interfaces del sensor y ver la página de resumen de la instalación del sensor.

34. El primer paso es el de seleccionar el método de actualización del conjunto de firmas en *Choose signature set update method*. Aquí es posible identificar el último conjunto de firmas disponible en el componente *Manager* y decidir si se necesita descargar el último juego de firmas del servidor de actualizaciones (*Update Server*). Para ello, hay que llevar a cabo las siguientes tareas:

    a) Indicar cómo obtener el último conjunto de firmas. En el panel se muestra la versión del conjunto de firmas actual disponible en el *Manager*:

        - *Importing Signature sets from a Local Directory* – Es posible importar el conjunto de firmas en el componente *Manager* desde un directorio local.
        - *Downloading the latest Signature set from McAfee Update Server* – Es posible descargar el ultimo conjunto de firmas desde *McAfee Network Security Update Server.*
        - *Skip Update Server authentication and signature set download* – Utilizar esta opción para continuar con el conjunto por defecto de firmas que se ha recibido a través de la instalación del componente Manager.

- Clic *Next.*

b) A continuación, es necesario obtener el último conjunto de descargas desde el *Update Server*:

- En la página *Choose signature set update method*, seleccionar la opción *McAfee Update Server*.
- Clic en *Next*. Se muestra la página *Authentication.*
- Introducir las credenciales (*Customer ID*/*Customer password*) proporcionadas por McAfee.
- Clic *Next.* Se lista el conjunto de firmas disponibles.
- Seleccionar el conjunto de firmas requerido y después hacer clic en *Next*. Se muestra la página *Signature set download status.*
- Clic en *Next* cuando la descarga esté completada. Una vez que el conjunto de firmas haya sido descargado, se mostrará la página *Add a Sensor*.
- El siguiente paso consiste en importar el conjunto de firmas desde un directorio local:
- En la página *Choose signature set update method*, seleccionar la opción *Import signature set from local directory*.
- Clic *Next*. Se mostrará la página *Import Attack Set.*
- Clic en *Browse* para seleccionar el fichero del directorio.
- Clic *Next*. Se mostrará la ventana *Import Status*.

c) Después de que el conjunto de firmas haya sido incluido, se muestra la página *Add a Sensor*. Para añadir un sensor es necesario seguir los siguientes pasos:

- Clic en *Devices* → *<Admin Domain>* → *Global* → *Add and Remove Devices.* Clic en *New*.
- Introducir los detalles relevantes en el diálogo *Add New Device*.
- Introducir el nombre del dispositivo (*Device Name*). El nombre del sensor debe de comenzar con una letra. La longitud máxima del campo es de 25 caracteres.
- Introducir el tipo de sensor entre las opciones soportadas: *IPS Sensor, Virtual HIP Sensor, NTBA Appliance,* o *Load Balancer*.

- Introducir el campo *Shared Secret*. Introducir de nuevo para confirmar. El "secreto compartido" debe de tener un mínimo de 9 caracteres. La clave no debe de empezar con un carácter de exclamación y no debe de tener ningún espacio. Los parámetros que se pueden utilizar para definir la clave son:
  - Caracteres, mayúsculas y minúsculas.
  - Dígitos.
  - Caracteres espciales (~ ` ! @ # $ % ^ & * ( ) _ + - = [ ] { } \ | ; : " ' , . <? /).
- Seleccionar el *Updating Mode* entre las opciones Online u Offline. El modo Offline (modo por defecto) habilita la actualización del sensor sin conexión y parará la configuración inicial de actualización del *Manager* al sensor cuando se establezca la relación de confianza entre ambos componentes. Es posible cambiar el modo a través del Manager navegando a *Devices|<Domain Name>|Global|Add and Remove Devices*. Seleccionar el sensor listado, hacer clic en *Edit* y, en la página de *Edit Device Information*, seleccionar *Online* u *Offline* a través de la opción *Updating Mode*. El estado del sensor será mostrado, del mismo modo que en la interfaz de comandos CLI, solo después de que la configuración se modifique correctamente.
- Rellenar los campos *Contact Information* y *Location* (ambos opcionales).
- Clic en *Save*.

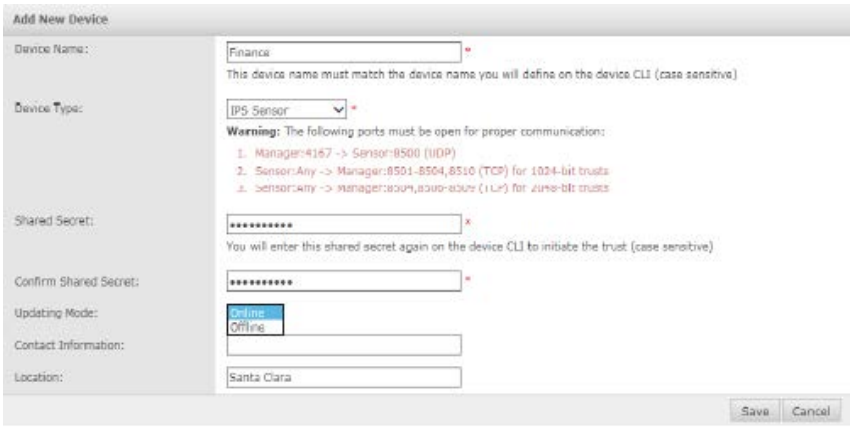

Ilustración 17. Panel para añadir un nuevo sensor

- Un cuadro de información confirmará que se ha añadido un sensor correctamente.

- Clic en *Next*.
- El nuevo sensor se lista en la página de Sensores. Se puede seleccionar el sensor y hacer clic en *Edit* para editar su configuración.

d) Es posible realizar la configuración del sensor mediante la interfaz de línea de comandos CLI. Esta tarea se realiza para establecer una cadena de confianza con el sensor.

- Realizar el primer inicio de sesión. Para ello, es necesario introducir las credenciales por defecto con nombre de usuario *admin* y contraseña *admin123*. **Se debe llevar a cabo un cambio de contraseña por razones de seguridad, siguiendo los requisitos de complejidad siguientes**:
  - Mínimo de 9 caracteres de longitud.
  - Utilización de mayúsculas, minúsculas, dígitos y caracteres especiales: ~ ` ! @ # $ % ^ & * ( ) _ + - = [ ] { } \ | ; : " ' , . <? /
- Establecer el nombre del sensor. Para ello, insertar el siguiente comando: *set sensor name <WORD>.* Este nombre es sensible a mayúsculas con más de 25 caracteres. La cadena debe de comenzar con una letra.
- Establecer la dirección IP y la máscara de subred en el sensor. En la interfaz, escribir: *set sensor ip <A.B.C.D> <E.F.G.H>.*
- Si el sensor no está en la misma red que el componente Manager, *establecer la dirección de la pasarela por defecto*. Para ello, introducir el comando: *set Sensor Gateway <A.B.C.D>.*
- Establecer la dirección IP del servidor *Manager*. Incluir el siguiente comando: *set Manager ip <A.B.C.D>.*
- Comprobar la configuración. Se recomienda realizar un *ping* desde el sensor hacia el *Manager* para determinar que la configuración, hasta este punto, se ha realizado correctamente. En caso de que no se pueda establecer, será necesario repetir los pasos anteriores para comprobar que la configuración es correcta.
- Establecer un valor de clave compartida para el sensor. Este valor es utilizado para establecer una relación de confianza entre el sensor y el *Manager*. Para ello, hay que utilizar el siguiente comando: set *Sensor sharedsecretkey*. El sensor después solicitará

la introducción de un valor de clave secreta compartida. Introducir un valor y volver a introducirlo para verificarlo.

- Modificar la contraseña por defecto del sensor. Es necesario introducir el siguiente comando: *passwd*. Automáticamente se solicitará la introducción de una nueva contraseña. La contraseña debe de cumplir la siguiente política de complejidad:
  - Mínimo de 9 caracteres de longitud.
  - Utilización de mayúsculas, minúsculas, dígitos y caracteres especiales: ~ ` ! @ # $ % ^ & * ( ) _ + - = [ ] { } \ | ; : " ' , . <? /
- Para terminar la sesión, introducir el comando: *exit*.
- Volver al asistente de instalación del sensor para continuar con la instalación del sensor. En este punto se observará la página *Discovery page*.
- Clic en *Next*.

e) Por último, se incluyen a continuación los requisitos mínimos para la instalación del producto:

	Minimum	Recommended
Operating system	• Windows 7, English or Japanese • Windows 8, English or Japanese • Windows 8.1, English or Japanese • Windows 10, English or Japanese The display language of the Manager client must be the same as that of the Manager server operating system.	
RAM	2 GB	4 GB
CPU	1.5 GHz processor	1.5 GHz or faster
Browser	• Internet Explorer 10, 11 • Mozilla Firefox • Google Chrome (App mode in Windows 8 is not supported) To avoid the certificate mismatch error and security warning, add the Manager web certificate to the trusted certificate list.	• Internet Explorer 11 • Mozilla Firefox 20.0 or later • Google Chrome 24.0 or later In Mozilla Firefox version 52 or Google Chrome version 42 and above, the NPAPI plug-in is disabled by default.

Ilustración 18. Requisitos mínimos permitidos en Windows

f) Estos requisitos mínimos han sido obtenidos directamente de los manuales de usuario del fabricante. No obstante, se recomienda no hacer uso de sistemas operativos sin soporte de seguridad (como Windows 7) ya que no dispondrá de las últimas actualizaciones de seguridad disponibles.

5 FASE DE CONFIGURACIÓN

5.1 MODO DE OPERACIÓN SEGURO

35. La configuración necesaria para que el producto opere de forma segura consiste en aplicar una **configuración segura del componente *Manager* y de los sensores** que se encuentren desplegados.

36. Es necesario llevar a cabo los siguientes pasos para configurar el componente *Manager* con el sistema operativo MLOS:

    a) Hacer inicio de sesión en la consola *Manager* haciendo uso de las credenciales por defecto:

        i. Nombre de usuario: *admin*

        ii. Contraseña: *MLOSnsmApp*

        iii. La contraseña por defecto de la consola Manager en *MLOSnscmApp*.

    b) El acceso mediante conexión SSH a la instancia virtual del Linux *Manager* no está soportada por la aplicación Putty. McAfee recomienda utilizar *Tera Term* para acceso remoto a la instancia MLOS Manager virtual utilizando SSH.

    c) Se debe modificar la contraseña. La nueva contraseña debe de tener al menos 9 caracteres de longitud y debe de tener una combinación de números, caracteres, y caracteres especiales.

    d) Para actualizar los parámetros de red, es necesario utilizar el comando *set network configuration*. Durante la ejecución del comando, se debe introducir los parámetros de red para la instancia del componente *Manager* tal como se muestra a continuación:

        i. Enter the DOMAIN NAME: <Manager_Domain_Name>

        ii. Enter the HOSTNAME: <Manager_Hostname>

        iii. Enter the IP ADDRESS: <Manager_IP_Address>

        iv. Enter the NETMASK: <Netmask_IP_Address>

        v. Enter the GATEWAY: <Gateway_IP_Address>

        vi. Enter the DNS1: <DNS1_Server_IP_Address>

        vii. Do you want to set DNS2 ? (y/n): <y/n>

        viii. Enter the DNS2: <DNS2_Server_IP_Address>

    e) Una vez terminada la ejecución del comando, se recomienda tomar nota de la dirección MAC mostrada.

f) Reiniciar la instancia virtual del *Manager* utilizando el comando *reboot*.

g) Para que el sistema se ejecute en modo evaluado, es necesario que tanto el *Manager* como los sensores usen certificados firmados por una CA para establecer confianza entre sí. El proceso de configuración se encuentra en la sección *5.6.GESTIÓN DE CERTIFICADOS*.

5.2 AUTENTICACIÓN

37. Los mecanismos de autenticación que utiliza el producto para autenticar a un usuario son los siguientes:

    a) Credenciales locales, mediante un usuario y contraseña de acceso.

    b) Autenticación mediante servidor externo RADIUS o LDAP.

    c) Las cuentas de usuario para el sensor pueden estar centralizadas y autenticadas mediante un servidor TACACS+ (*Terminal Access Controller Access Control System plus*).

5.3 ADMINISTRACIÓN DEL PRODUCTO

5.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

38. El administrador de sistema puede llevar a cabo la administración del producto mediante la interfaz gráfica de administración del *Manager* accediendo a la siguiente URL mediante HTTPS:

    https://<hostname or host-IP>

39. Es posible acceder a la interfaz de administración *Manager* a través de SSH con una autenticación mediante *public key* y hacer uso de comandos CLI. Las instrucciones que pueden ejecutarse se pueden consultar en la sección "CLI COMMANDS" en la guía [REF1].

40. Adicionalmente, los administradores pueden acceder a la interfaz de administración *Manager* con *Smart Cards* tales como CAC (*Common Access Card*) o PIV (*Personal Identification Verification*). Para ello, es necesario que la máquina que se conecta a la interfaz de administración disponga de un lector de *Smart Card*s. Igualmente, el proceso de autenticación requiere de un PIN asociado a la *Smart Card*. Para habilitar la autenticación CAC es necesario seguir los siguientes pasos:

    a) Iniciar sesión en la interfaz gráfica del componente *Manager*.

    b) Ir a *Manager* → *<Admin domain Name>* → *GUI Access* → *CAC Authentication*.

c) En la sección *Enable*, configurar la autenticación CAC rellenando los campos incluidos.

d) Clic Save.

e) Iniciar sesión en la consola del componente *Manager*.

f) Detener el servicio haciendo uso del comando *manager stop*.

g) Reiniciar el servicio utilizando el comando *manager start*.

41. Una vez configurado, es posible iniciar sesión a partir de los siguientes pasos:

a) Insertar una tarjeta en el lector.

b) Iniciar una nueva sesión en el navegador para iniciar el *Manager*. Aparecerá una ventana para elegir el certificado CAC/PIV.

c) Seleccionar el certificado. Se solicitará insertar un PIN.

d) Introducir el PIN. Se permitirá un máximo de 3 intentos para introducirlo antes de bloquear al usuario. No es posible desbloquear una tarjeta CAC/PIV y deberá de ser reemplazada.

e) Si la autenticación es exitosa, se proporcionará acceso a la página principal del componente *Manager*.

5.3.2 CONFIGURACIÓN DE ADMINISTRADORES

42. En la plataforma de *McAfee Network Security* los componentes del sistema se agrupan de forma lógica en *admin domains*; dentro de cada *admin domain*, los permisos/privilegios para ejecutar tareas y servicios dependen del rol otorgado a cada usuario. Existen los siguientes roles de administrador:

a) **ePO Dashboard Data Retriever:** tiene derechos para recopilar información del *McAfee Network Security Platform* al *McAfee ePO* (en caso de estar desplegado en una red) para mostrar información.

b) ***NOC Operator*:** monitoriza el entorno de seguridad.

c) ***Policy Administrator***: gestiona el sistema de prevención de intrusiones.

d) ***Report Generator***: capaz de generar y ejecutar informes.

e) ***Security Expert*:** gestiona las políticas de intrusión a través de la administración de IPS y NTBA.

f) ***Super User:*** dispone de todos los privilegios en el *admin domain* y en todos los subdominios de este, además de poder crear o eliminar otros *Super Users* en el *admin domain*.

g) ***System Administrator***: pertenece a la administración del propio sistema, gestionando la interfaz *Manager* y la lista de dispositivos. Administra el *software* y el rendimiento del sistema; además de añadir, configurar y eliminar sensores gestionando, además, los errores del sistema.

43. Para asignar un rol a un usuario es necesario seguir los pasos a continuación:

    a) En la interfaz gráfica de administración seleccionar *Manager* → *<Admin Domain Name>* → *Users and Role* → *Role Assignments.*

    b) Seleccionar un usuario en la tabla *Role Assignment*.

    c) Acceder al rol del usuario en el campo *Roles (current domain).* Si el usuario no dispone de ningún rol asignado el campo estará vacío.

    d) Pulsar *Edit* → *New Assignment* → y seleccionar el *admin domain* sobre el que añadir el rol al usuario.

    e) Seleccionar el rol/es a asignar al usuario y pulsar *Save*.

44. El usuario *System Administrator* puede configurar una política de contraseña accediendo a *Manager* → *<Admin Domain Name>* → *Setup* → *GUI Access* → *Password Control*. La configuración de una política de contraseñas es recomendable para garantizar que cada usuario que tenga acceso a la interfaz del producto cumpla con los requisitos de complejidad de la contraseña suficientes para considerarla como segura.

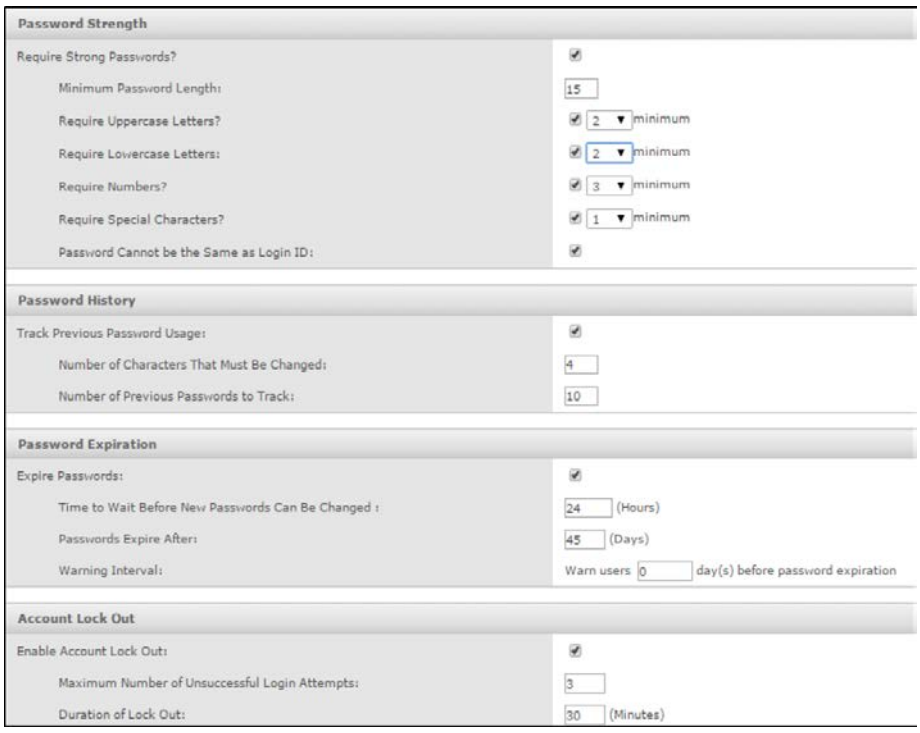

Ilustración 19. Panel de gestión de políticas de contraseña

45. Se recomienda cumplir con las siguientes directrices y opciones de configuración para la política de contraseñas:

    a) Deberán ser de 9 caracteres como mínimo, incluyendo mayúsculas y minúsculas, caracteres numéricos y caracteres especiales. Además, se debe activar la opción "*Password Cannot be the Same as Login ID*" para evitar que se incluya el *Login ID* como parte de la contraseña.

    b) Se deberá establecer un límite de vigencia y expiración de las contraseñas de máximo 180 días.

    c) Para evitar que las contraseñas se repitan se debe configurar el número mínimo de caracteres que se debe cambiar respecto a contraseñas anteriores y el número de contraseñas previas a comprobar. Una recomendación es la de situar este valor en un mínimo de 10.

    d) Se deberá configurar el número máximo de inicios de sesión y la duración de un tiempo de *Lock Out*. Se recomienda un número máximo de 3 inicios de sesión fallidos y una duración de *Lock Out* no superior a 30 minutos.

46. Se recomienda configurar el *TimeOut* de inactividad de sesión en 15 minutos y el número de sesiones concurrentes a 1.

47. Se debe configurar un *banner* de *login*. McAfee NSP permite añadir un banner que contenga una imagen de tipo .jpeg o .png con un tamaño de 100x35 píxeles, además de texto personalizado. Para ello hay que acceder a la pestaña de Logon *Banner*, a través de *Manager* → *<Admin Domain Name>* → *Setup* → *GUI Access* → *Logon Banner.*

5.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

5.4.1 CONFIGURACIÓN DE SERVICIOS

48. Se debe configurar el uso de un *firewall* en el servidor *Manager*. Además, debe configurarse un *packet-filtering Firewall* para bloquear las conexiones a los puertos 8551, 8552, 3306, 8007 y 8009 del servidor *Manager*. El objetivo es **denegar todas las conexiones que no son inicializadas** desde el *localhost*, es decir, del mismo servidor Manager.

49. Se usan ciertos puertos para la comunicación entre los sensores y el *Manager*, todos los demás **puertos innecesarios deben cerrarse** por razones de seguridad.

50. Para garantizar la integridad del sistema **debe deshabilitarse el uso de USB externos**. Para ello, es necesario acceder a una *shell* de Manager, entrar en *private mode*, ejecutar "*edit blacklist*.conf", añadir "*blacklist usb-storage*" y guardar los cambios.

51. Para reducir la superficie de ataque es necesario **deshabilitar el *admin access* en los sensores una vez han sido inicializados** y se ha creado una situación de confianza con el *Manager*. Esto se consigue accediendo a través de SSH a cada sensor y ejecutando la siguiente instrucción: *disableadminaccess*.

5.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

52. El IPS hace uso de protocolos de comunicaciones seguras en los siguientes casos:
    a) Intercambio de información de configuración.
    b) Sincronización de hora/fecha desde los sensores NSM.
    c) Transferencia de información IPS hacia los sensores NSM.
    d) Transferencia de registros de auditoría hacia los sensores NSM.
    e) Distribución de actualizaciones hacia los sensores.
53. Las conexiones entre sensores NSM/NS y las conexiones entre sensores NSM y el servidor de auditoría están cifradas usando TLS 1.2 por defecto.
54. El producto está configurado por defecto para evitar que la versión 1.2 del protocolo TLS no pueda ser modificada. Para ello, en las comunicaciones que se establecen entre los sensores NSM/NS y las conexiones entre los sensores NSM y el servidor de auditoría del producto se deniega cualquier conexión que solicite un diente a través de SSL 2.0, SSL 3.0, TLS 1.0 y TLS 1.1. De esta forma la conexión mediante el protocolo de comunicación TLS 1.2 la única permitida.
55. Las sesiones entre la estación de administración y el producto están protegidas usando SSH (OpenSSH v7.8) o HTTPS.
56. Se usan los siguientes algoritmos para proteger las conexiones entre los servicios del NSP con otras entidades:
    a) AES CBC (128 y 256 bits) y AES GCM (128 y 256 bits) para el cifrado simétrico y confidencialidad de la información.
    b) SHS con modos: SHA-1, SHA-256, SHA-384 y SHA-512.
    c) DRBG (*Deterministic random bit generation*), algoritmo auxiliar de AES.
    d) ECDSA para la generación de claves (P-256, P-384).
    e) RSA para generación de claves (n-2048) y generación y verificación de firmas (SHA-256, SHA-512).
    f) HMAC como algoritmo auxiliar (SHA-1, SHA-256, SHA-384, SHA-512), para proporcionar integridad a la comunicación.

g) KAS ECC (P-256, P-384).

57. Como se puede observar, varios algoritmos tienen la posibilidad de hacer uso de **SHA-1**, el cual no es recomendable ya que es considerado como inseguro y, por tanto, **debe deshabilitarse**. Para ello, se deben seguir los siguientes pasos:

    a) Acceder al archivo *Server.xml* que se encuentra en el directorio *"Apache-tomcat\config".* En el puerto 443 reemplazar el valor del algoritmo de cifrado con:

    ciphers="TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256"

    b) Acceder al archivo *java.security* que se encuentra en los directorios *"/config"* y en *"jre/lib/security"*. Reemplazar la propiedad *"jdk.tls.disabledAlgorithms"* con:

    jdk.tls.disabledAlgorithms=anon, NULL, DHE, DESede, ECDH, ECDSA, SHA1, SSLv3, RC4, MD5withRSA, CBC, DH keySize < 768, EC keySize < 224

5.6 GESTIÓN DE CERTIFICADOS

58. El NSM puede administrar sensores que usen certificados X.509 auto firmados durante la instalación y testeo. Todos los sensores deben usar certificados firmados por una Autoridad de Certificados (CA).

5.6.1 ADMINISTRACIÓN DE CERTIFICADOS PARA EL MANAGER Y LOS SENSORES

59. El *Manager* y los sensores usan certificados SSL para establecer una conexión TLS. Por defecto, el Manager y los sensores usan certificados auto firmados para establecer confianza entre ellos. Sin embargo, como se ha comentado, se deben utilizar certificados firmados por una CA tales como *Verisign, Geotrust*, etc. para establecer una cadena de confianza entre los componentes *Manager* y los sensores.

60. Para administrar los certificados del *Manager* es necesario acceder a *Manager* → *<Root Admin Domain>* → *Setup* → *Certificates.* Para administrar los certificados del sensor es necesario acceder a *Devices* → *<Root Admin Domain>* → *Devices* → *<Device Name>* → *Setup* → *Trust Certificates*.

Opción	Definición
Active Certificate	Muestra el tipo de certificado activo, autofirmado o firmado por una CA.
Self-Signed Listening Ports	Puertos utilizados por el componente *Manager* para establecer confianza con el sensor cuando

	ambos utilizan certificados autofirmados.
CA-Signed Listening Ports	Puertos utilizados por el componente *Manager* para establecer confianza con el sensor cuando ambos utilizan certificados firmados por una CA.

Tabla 1. Parámetros de configuración de certificados

61. En la sección de "*Certificate Status*" se dispone de la opción de cambiar el certificado activo para los sensores. Se puede cambiar de un certificado auto firmado a uno firmado por una CA y viceversa. En la sección de *"CA-Signed Certificate"* es posible visualizar los datos correspondientes del certificado, como el *Common Name, Organization, Department, City, Issued By,* etc.

5.6.2 SOLICITUD DE CERTIFICADOS FIRMADOS POR UNA CA

62. El primer paso a seguir antes de solicitar un certificado firmado por una CA es generar un CSR (*Certificate Signing Request*). Para ello, en el componente Manager se accederá a *Manager → <Root Admin Domain> → Setup → Certificates* y para el caso del sensor se accederá a D*evices → <Root Admin Domain> → Devices → <Device Name> → Setup → Trust Certificates.*

63. En la sección "*CA-Signed Certificate*" pulsar sobre *Generate CSR*. Luego, se abrirá una ventana llamada "*Generate CSR*" donde hay que introducir los siguientes datos:

    a) ***Common Name*****:** Nombre de dominio del servidor. Este campo no puede contener caracteres *wildcard* tales como '*' o '?' o protocolos como https:// o http://.

    b) ***Organization***: El nombre legal de la organización.

    c) ***Department***: Es un campo optativo.

    d) ***City***: La ciudad donde se encuentra la organización.

    e) ***State/Province***: Estado o provincia donde se encuentra la organización.

    f) ***Country***: País donde se encuentra la organización.

    g) ***Key Size***: Tamaño de la clave RSA, 2048 bits de longitud por defecto.

    h) ***Subject Alternative Name***: La IP del servidor. Es un campo no editable.

64. Una vez generado el CSR, se debe exportar desde la opción *Export CSR*. El CSR se exporta al directorio de descargas de la máquina remota que está accediendo al *Manager*. Con el archivo CSR se puede solicitar un certificado a una CA a elección. Una vez recibido el certificado firmado por una CA, este debe ser importado.

65. **Se deben utilizar de certificados firmados por una CA que utilicen algoritmos autorizados según la guía CCN-STIC-807, como SHA256 y RSA 2048 bits.**

5.7 SERVIDORES DE AUTENTICACIÓN

66. El producto permite llevar a cabo la configuración de dos (2) tipos de servidores de autenticación externos: RADIUS y LDAP.

67. En las siguientes subsecciones se llevará a cabo una descripción del proceso a seguir para realizar la configuración de cada uno.

5.7.1 SERVIDOR DE AUTENTICACIÓN LDAP

68. El Protocolo de Acceso a Directorios Ligeros (*Lightweight Directory Access Protocol* – LDAP) es un conjunto de protocolos para acceder a directorios de información.

69. Es posible configurar un servidor LDAP desde el componente Manager, hasta un máximo de cuatro (4) servidores LDAP. Si el primer servidor LDAP no está disponible para la comunicación, debido a un fallo en la red, se intentará establecer una comunicación con el segundo o tercer servidor. Si la autenticación falla en cualquier servidor disponible, entonces el componente *Manager* no se comunicará con otros servidores. Se debe configurar un servidor LDAP con el protocolo SSL habilitado. Antes de habilitar SSL, es necesario realizar los siguientes pasos para confirmar si LDAP sobre SSL está funcionando en el servidor de *Active Directory:*

    a) En el sistema operativo Windows, en el menú de *Inicio,* seleccionar *Ejecutar*.

    b) Introducir *ldp.exe* y presionar *ENTER.* Se puede observar una nueva ventana denominada *Ldp.*

    c) Hacer clic en *Conexión.* Se abre un dialogo *Conectar.*

    d) Introducir el *Fully Qualified Domain Name (FQDN)* del servidor de *Active Directory* utilizado para generar el certificado en el campo de *Servidor*.

    e) Seleccionar SSL. Confirmar que el puerto es 636, después hacer clic en OK.

70. Una vez realizados estos pasos previos, es posible configurar LDAP sobre SSL en el producto mediante los siguientes pasos:

    a) Seleccionar *Manager* → *<Admin Domain Name>* → *Setup* → *External Authentication* → *LDAP.*

    b) Clic en *New*. Se mostrará la página *Ad dan LDAP Server*.

c) Actualizar los siguientes campos para completar el proceso de inclusión de un nuevo servidor LDAP:

Opción	Definición
Enable LDAP Authentication?	Seleccionar *Yes* para continuar añadiendo el servidor LDAP.
Enable SSL?	Seleccionar el cuadro de texto para habilitar el cifrado SSL. Se debe de importar el certificado SSL del servidor LDAP en el almacén de claves del componente Manager para su autenticación. Para más información, véase *5.6.GESTIÓN DE CERTIFICADOS*
LDAP Server Name or IP Address	Introducir la dirección IPv4 o IPv6 del servidor LDAP.
Server Port	Introducir el número de puerto entre 0 y 65535. El puerto por defecto es 636.
Test Connection	(Opcional) Clic para verificar que el componente Manager puede conectarse al servidor LDAP.
Save	Clic para guardar los cambios.
Cancel	Clic para cancelar los cambios y salir.

Tabla 2. Parámetros de configuración de LDAP

5.7.2 SERVIDOR DE AUTENTICACIÓN RADIUS

71. El Servicio de Autenticación Remota de usuarios (RADIUS, *Remote Authentication Dial In User Service*) es un protocolo AAA (*Authentication, Authorization and Accounting*) para aplicaciones relacionadas con el acceso a la red.

72. Mientras que se realiza la conexión a Internet, se requerirá la inserción de un nombre de usuario y contraseña. La información se pasa a través de un dispositivo de acceso a la red para, posteriormente, pasar la información a un servidor RADIUS. El servidor RADIUS comprueba si la información es correcta utilizando esquemas de autenticación como PAP, CHAP y EAP-MD5. Si se acepta, el servidor autorizará el acceso.

73. Utilizando el componente *Manager*, es posible configurar un servidor RADIUS, hasta un máximo de 4 servidores RADIUS. Si el primer servidor RADIUS no está disponible para la comunicación, debido a un fallo en la red, el componente Manager intentará comunicarse con el segundo o tercer servidor. Si la

autenticación falla en cualquier servidor disponible, entonces el componente *Manager* no se comunicará con otros servidores disponibles.

5.8 SINCRONIZACIÓN HORARIA

74. Varias características de seguridad del dispositivo, además del registro, están fuertemente ligadas a la hora del sistema. Debido a ello, es de vital importancia que el **servidor Manager cuente con una fuente de tiempo de confianza**.

75. Para configurar la sincronización horaria a través de NTP en el Manager es necesario:

    a) *Log in* en la *shell* de *Manager*.

    b) Parar el protocolo NTP usando la instrucción *"ntp stop".*

    c) Configurar el protocolo NTP usando la instrucción *"set network ntp <NTP server Domain Name/IP Address>".*

    d) Iniciar el protocolo NTP usando la instrucción *"ntp start".*

    e) Entrar en el modo privado.

    f) Editar el archivo *"/etc/ntp.conf"* y añadir o actualizar con la siguiente línea: *"server 0.rhel.pool.ntp.org iburst maxpoll 10".*

    g) Salir del modo privado.

    h) Reiniciar el protocolo NTP usando las instrucciones "*ntp stop"* y *"ntp start".*

5.9 ACTUALIZACIONES

76. Para que el sistema pueda detectar y proteger la red de actividad maliciosa, **el componente *Manager* y los sensores deben estar actualizados.** Las actualizaciones y parches de seguridad están disponibles en el componente *McAfee Network Security Update Server.*

77. Se pueden obtener estas actualizaciones del *Update Server*:

    a) Conectándose directamente al *Update Server* desde el servidor *Manager*.

    b) Conectándose al *Update Server* a través de un *proxy server*.

    c) Conectándose al *Update Server* desde un *Manager Client*, descargar las actualizaciones y luego importando estas al servidor Manager. Esta es la manera más segura, ya que el servidor Manager no se conecta a Internet.

    d) Conectándose al Update *Server* desde un *Manager Client* y descargando las actualizaciones a un servidor TFTP y subiendo estas a los sensores usando

una interfaz de línea de comandos (CLI). Este método solo funciona para actualizaciones de sensores.

78. Una vez descargadas las actualizaciones, el Manager transferirá a los sensores las actualizaciones diseñadas para estos.

79. Existen diversas formas de realizar el proceso de actualización:

    a) Actualización automática del *Manager* y actualización manual del *Manager* a los sensores. Esta opción permite al *Manager* recibir actualizaciones automáticamente, pero permite al administrador elegir las actualizaciones a aplicar a los sensores.

    b) Actualización manual del Manager y actualización automática del Manager a los sensores. Esta opción permite elegir al administrador que actualizaciones descargar, pero una vez descargadas se aplican automáticamente en los sensores.

    c) Actualización manual completa. Esta opción permite elegir al administrador qué actualizaciones aplicar y cuándo hacerlo en los sensores.

    d) Actualización automática completa. Esta opción actualiza el Manager y los sensores de forma automática, sin intervención del administrador.

    e) Actualización en tiempo real. Esta opción es parecida a la actualización automática completa, pero en lugar de esperar a un intervalo de tiempo programado, hará la actualización nada más esté disponible en el *Update Server.*

5.10 SNMP

80. Se usa de forma predeterminada SNMPv3 entre el componente Manager y los sensores. Si la confianza generada entre el Manager y el sensor se ha establecido mediante un certificado firmado por una CA, el sensor usará el puerto 18500 como un servidor TLS para ofrecer SNMPv3; si, por el contrario, el certificado usado para establecer confianza es auto-firmado, el sensor usará el puerto 8500 como un servidor TCP/UPD para ofrecer SNMPv3.

81. Si existe un *firewall* entre el servidor *Manager* y los sensores, es necesario abrir en el *Manager* los puertos UDP 4167 (*Command Channel*) y 162 (*SNMP Forwarding*).

5.11 ALTA DISPONIBILIDAD

82. Los sensores admiten implementar alta disponibilidad utilizando *stateful fail-over* entre dos (2) sensores idénticos. Los sensores están interconectados, copian el

tráfico entre ellos y mantienen la sincronización. Si uno de los sensores falla, el sensor en espera toma automáticamente el relevo y continúa supervisando el tráfico sin perder el estado de la sesión ni afectar al nivel de protección.

83. La plataforma de seguridad de la red también admite la recuperación de desastres del gestor (MDR) para su consola de gestión. Si, por cualquier motivo, el *McAfee Network Security Manager* principal se desconecta, el secundario puede ocupar automáticamente su lugar, procesando las alertas y gestionando la configuración de los sensores.

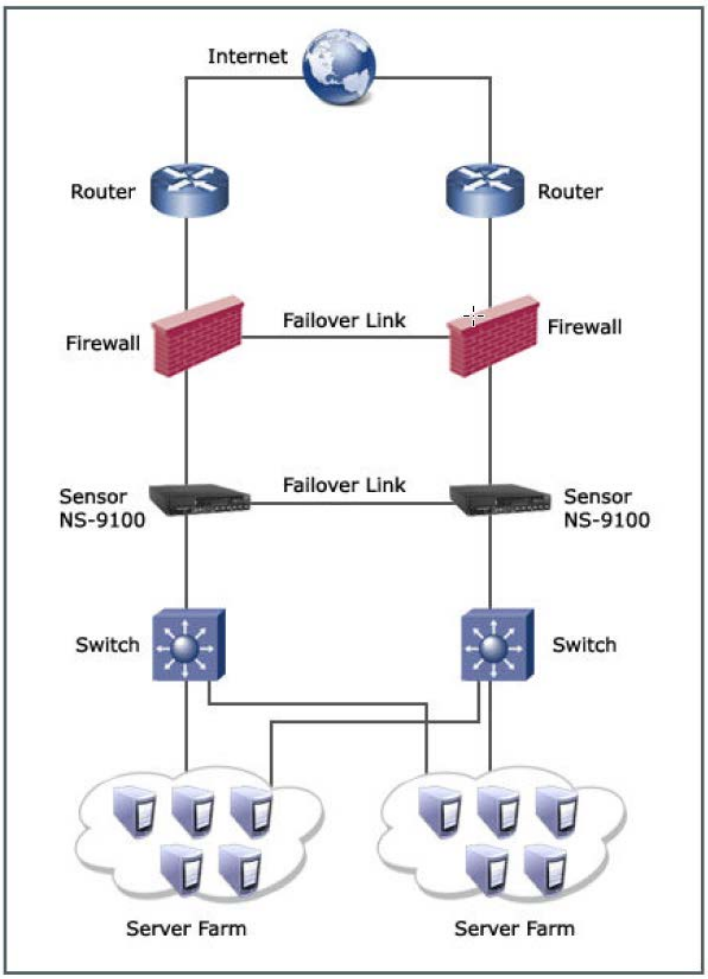

Ilustración 20. Esquema de alta disponibilidad

84. Con MDR, se despliegan dos (2) servidores Manager como parte del NSP. Uno de los hosts se configura como sistema principal y el otro como secundario. Cada uno de ellos utiliza la misma versión principal del software *Manager* con bases de datos duplicadas; sin embargo, no es necesario que la configuración de hardware de los dos hosts sea idéntica. El *Manager* Secundario puede ser desplegado en cualquier lugar, por ejemplo, en una localización de recuperación de desastres, alejada del *Manager* principal.

85. El *Manager* principal es el que se encuentra activo por defecto; este se comunica con el *Update Server*, envía los datos de configuración a los sensores, y recibe las alertas de los sensores. El *Manager* secundario permanece en estado de espera por defecto. Mientras está en modo de espera, monitorea el estado de salud del *Manager* primario y recupera la información de configuración de los sensores desde el *Manager* primario a intervalos de tiempo configurados. Para realizar la activación del MDR es suficiente con activar la opción *MDR* del menú *Setup* y rellenar los siguientes campos:

    a) ***Role of this Manager.*** Seleccionar *Primary* para utilizar el Manager como principal o *Secondary* para utilizarlo como respaldo.

    b) ***Use Out-of-Band (OOB) Manager-to-Manager Communication?*** Seleccionar *Yes* para separar las interfaces de comunicación de los Manager y la comunicación entre Manager y sensor. Seleccionar la opción *No* para que se haga uso de la misma interfaz para ambos canales de comunicación.

    c) ***Peer IP for Manager-to-Manager Communication.*** Esta opción aparece si se selecciona la opción *Yes* en el campo anterior.

    d) ***Peer IP for Manager-to-Sensor Communication*.** Introducir la dirección IP en el componente *Manager* utilizado para la comunicación con el sensor.

    e) ***MDR Pair Shared Secret.*** Debe compartise la misma clave secreta en ambos *Managers* para que la activación del MDR sea exitosa. Es necesario introducir un mínimo de 8 caracteres y no utilizar caracteres especiales.

    f) ***Confirm MDR Pair Shared Secret.*** Introducir la misma clave secreta compartida.

    g) ***Downtime Before Switchover.*** Introducir el tiempo en minutos que debe de transcurrir en caso de que el componente *Manager* principal caiga, para que el *Manager* secundario comience su tarea de respaldo.

5.12 AUDITORÍA

5.12.1 REGISTRO DE EVENTOS

86. En el sistema se producen alertas, algunas de ellas llevan asociadas a los registros de auditoría. Estos contienen eventos relacionados con la administración del *Manager*, los sensores y los eventos de seguridad entre otros. Existen varios tipos de logs:

    a) ***Attack Log*** → guarda información de los ataques producidos contra la infraestructura, listando primero el más reciente.

b) ***System Log*** → guarda información del propio *Manager*. Los logs se encuentran en *<Network Security Manager Directory>/app/<all log files>*.

c) ***Packet log*** → guarda información de eventos en la red/infraestructura captados por los sensores y sus políticas de configuración.

d) ***Fault log*** → guarda los detalles de las autenticaciones fallidas en el Manager.

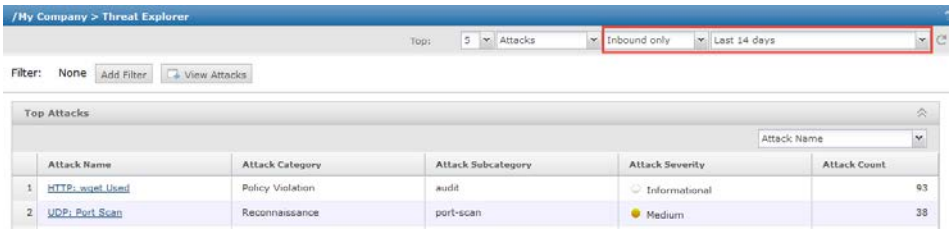

Ilustración 21. Ejemplo de Attack Log

5.12.2 ALMACENAMIENTO

87. El almacenamiento local se realiza en el servidor Manager, el cual guarda los logs del sistema, los de ataque, los de autenticación fallida; además de recibir los logs por parte de los sensores. El almacenamiento local máximo depende de la capacidad de almacenamiento del servidor *Manager*.

88. Se recomienda archivar logs cada cierto periodo de tiempo dependiendo del volumen de logs semanales; en una situación media se recomienda archivar logs cada 90 días.

89. Un punto de referencia para determinar la capacidad de almacenamiento necesaria de la base de datos que contendrá los logs y alertas es: calcular el volumen de alertas y logs que recibe el sistema de forma semanal y multiplicar este número por 52 (semanas que tiene el año). El tamaño medio de las alertas y logs es tal que así:

    a) Alertas sin log = 200 bytes (tamaño medio).

    b) Alertas con log = 650 bytes (tamaño medio).

Alerts/Week	DB Size (One Year) in GB
10,000	0.3
50,000	1.7
100,000	3.3
200,000	6.7
500,000	16.7
1,000,000	33.4
30,000,000	1002

Ilustración 22. Alertas recibidas por semana, y el espacio necesario de disco

90. El producto también permite realizar el envío de todos los registros de auditoría a un servidor *syslog* a través de una conexión segura TLS en tiempo real que es iniciada por el NSM. Si la conexión con el servidor *syslog* no está disponible, el producto sigue registrando los registros de auditoría en la base de datos local; sin embargo, los registros generados mientras que el servidor *syslog* no esté disponible no se transmitirán. Los 50000 registros de auditoría más recientes se conservan en el NSM; los registros de auditoría más antiguos se eliminan. Los sensores del producto envían sus registros de auditoría al NSM, donde se consolidan con los registros generados por el NSM y se envían al servidor *syslog*.

91. Para configurar la opción de exportar los registros de auditoría a un servidor *syslog* es necesario seguir los siguientes pasos:

    a) Seleccionar *Devices → <Admin Domain Name > → Global → IPS Device Settings → IPS Event Logging.*

    b) Rellenar los campos que se muestran. Será necesario habilitar la configuración, incluir la dirección IP del servidor *syslog*, establecer la priorización de los registros de auditoría y definir un mapeo de prioridad en función de la gravedad del evento detectado.

    c) También es posible configurar los parámetros de filtrado para generar notificaciones en función del tipo de ataque detectado.

    d) Finalmente, se puede seleccionar el tipo de mensaje que se mostrará en cada notificación en función de las necesidades de cada usuario.

92. El producto también permite configurar que los sensores desplegados envíen notificaciones de alerta al servidor *syslog*. Para ello, es necesario acceder al menú ***Devices → <Admin Domain Name > → Devices → <Device name> → Setup → Logging → IPS Event Logging*** y activar el campo ***Inherit Settings*** para rellenar los campos mencionados anteriormente.

5.13 BACKUP

93. Proteger la base de datos del producto de fallos de *hardware* o *software* es esencial para la integridad de la información. McAfee *NSP* permite generar *Back-ups* accediendo a ***Manager → <Admin Domain Name> → Maintenance → Database Backup*** o a través de la herramienta "***Database Backup and Restore Tool***", localizada en *"<Manager installation directory>\App\bin\dbadmin.bat"*.

94. Cuando se ejecuta un *back-up* se pueden guardar las siguientes tablas:

a) Todas las tablas: Realiza un *back-up* de toda la información, incluyendo configuraciones, alertas, auditorías. **Se recomienda hacer un *back-up* de todas las tablas mensualmente.**

b) Tablas de configuración: Realiza un *back-up* solo de las tablas que contengan tareas configuradas. **Se recomienda hacer un *back-up* de las tablas de configuración semanalmente**.

c) Tablas de auditoría: Realiza un *back-up* solo de la información de la actividad de los usuarios y las alertas. Es útil para realizar análisis offline.

d) Tablas de eventos: Realiza un *back-up* de alertas, *packet logs*, *hosts* y eventos de rendimiento de sensores.

e) Tablas de tendencia: Realiza un *back-up* de patrones de comportamiento (diarios, semanales y mensuales) sobre alertas y rendimiento de sensores.

95. **Se debe configurar la realización de back-ups automáticos de forma periódica.** Esto se consigue a través de *Manager* → *<Admin Domain Name>* → *Maintenance* → *Database Backup* → *Automated Backups*. Se debe seleccionar el destino del almacenamiento del back-up, su frecuencia y las tablas a guardar.

5.14 SERVICIOS DE SEGURIDAD

96. En el NPS todos los servicios, incluido el IPS, son *policy-based*. Por ejemplo, para IDS/IPS se usan políticas IPS y políticas de reconocimiento; para el servicio de *firewall* se usan políticas de *firewall* y así con los demás servicios. Generalmente, una política de seguridad es un conjunto de reglas que definen qué actividad deben detectar los sensores y cómo reaccionar ante esta. Existen las siguientes políticas de seguridad en el NSP:

a) Políticas de IPS

b) Políticas de reconocimiento

c) Políticas de *Malware* avanzado

d) Políticas de opciones de inspección

e) Políticas de *Firewall*

f) Políticas de *QoS*

g) Políticas de limitación de conexiones

97. Los componentes principales de una política IPS son un conjunto de *attack profiles* y sus definiciones. Ejemplo: definiciones de ataque a protocolos (HTTP, UDP), sistemas operativos, y demás información que circula por la red. Se

recomienda crear diferentes políticas IPS, cada una centrada en un problema específico o en un segmento determinado de la red.

98. Los ataques son clasificados según su tipo, por ejemplo, un ataque puede ser un *exploit*, un reconocimiento no autorizado sobra la red y los servicios, una denegación de servicios o una violación de políticas. Es necesario contar con un sensor en modo *inline* para rechazar y bloquear ataques. Existen varias formas de bloquear el tráfico malicioso:

    a) Bloquear *exploits* a través de políticas IPS.

    b) Bloquear tráfico *DoS* a través de detección de comportamiento.

    c) Bloquear la descarga de *malware* a través de políticas.

    d) Bloquear tráfico sospechoso a través de ACLs, en las políticas de *firewall*.

    e) Bloquear paquetes que violen el flujo TCP a través de la característica de normalización del NSP.

    f) Bloqueo de paquetes *IP-spoofed*; esto debe configurarse manualmente.

5.14.1 CREACIÓN DE UN *ATTACK SET PROFILE* (IPS)

99. Se recomienda la creación de políticas IPS para prevenir la intrusión de agentes externos en la red. Para configurar un *attack set profile* asociado a una política hay que acceder al *Manager* → *Policy* → *Domain* → *Intrusion Prevention* → *Objects* → *Attack Set Profiles*.

	Name	Description	Ownership and Visibility		Last Updated	
			Owner Domain	Editable Here	Time	By
1	Default Detection	The standard attack set (blocking disabled)	/My Company	No	Oct 05, 2016 11:43:37	admin
2	Default DoS and Reconnaissance Only	Threshold, learning and correlation-based attacks only (blocking disabled)	/My Company	No	Oct 05, 2016 11:44:47	admin
3	Default Exclude Informational	All attacks except informational-severity attacks (blocking disabled)	/My Company	No	Oct 05, 2016 11:44:35	admin
4	Default Prevention	The standard attack set (blocking enabled for RfSB attacks only)	/My Company	No	Oct 05, 2016 11:44:48	admin
5	Default Testing	All attacks (blocking disabled)	/My Company	No	Oct 05, 2016 11:44:41	admin
6	DMZ	Include all except for protocols TFTP, TELNET, RIP, NETBIOS, NFS, WINS, a...	/My Company	No	Oct 05, 2016 11:43:59	admin
7	DNS Server	Include only attacks for protocol DNS, generic backdoors, DOS and Reconn...	/My Company	No	Oct 05, 2016 11:44:21	admin
8	File Server	Include only attacks for protocols DNS, NFS, RPC, NETBIOS, SMB, generic ...	/My Company	No	Oct 05, 2016 11:44:28	admin
9	Inside Firewall	Include all except for protocols TFTP, TELNET, RIP, and excluding known no...	/My Company	No	Oct 05, 2016 11:44:05	admin
10	Internal Segment	Include all except for RIP, and excluding known noisy signatures.	/My Company	No	Oct 05, 2016 11:44:08	admin
11	Linux Server	Include all attacks where impacted OS includes Linux, and excluding known...	/My Company	No	Oct 05, 2016 11:44:31	admin
12	Mail Server	Include only attacks for protocols DNS, SMTP, POP3, and IMAP, generic back...	/My Company	No	Oct 05, 2016 11:44:19	admin
13	Outside Firewall	Include all except for the RECONNAISSANCE category, and excluding know...	/My Company	No	Oct 05, 2016 11:43:44	admin
14	Solaris Server	Include all attacks where impacted OS includes Solaris, and excluding know...	/My Company	No	Oct 05, 2016 11:44:30	admin
15	Unix Family	Include all attacks where impacted OS includes all Unix; and excluding kno...	/My Company	No	Oct 05, 2016 11:44:56	admin
16	Unix Server	Include all attacks where the impacted OS includes Unix, and excluding kno...	/My Company	No	Oct 05, 2016 11:44:32	admin
17	Web Server	Include only attacks for protocols DNS, HTTP, and FTP, generic backdoors, ...	/My Company	No	Oct 05, 2016 11:44:12	admin
18	Windows And Solaris Server	Include all attack where impacted OS includes Windows or Solaris, and excl...	/My Company	No	Oct 05, 2016 11:44:34	admin
19	Windows And Unix Server	Include all attacks where impacted OS includes Windows or Unix, and exclu...	/My Company	No	Oct 05, 2016 11:44:33	admin
20	Windows Family	Include all attacks where impacted OS includes all Windows versions; and e...	/My Company	No	Oct 05, 2016 11:44:54	admin
21	Windows Server	Include all attacks where impacted OS includes Windows servers, and exclu...	/My Company	No	Oct 05, 2016 11:44:30	admin

New Copy Edit Delete

Ilustración 23. Sección "Attack Set Profiles"

100. En este punto hay que pulsar sobre *New*, accediendo a la ventana de propiedades. Tras rellenar los campos de la ventana de propiedades (nombre, descripción, autor…) se accede a la ventana "*Attacks to Include/Exclude*" donde se puede incluir ataques a detectar y las acciones a tomar. El NPS cuenta con una serie de '*Attack sets*' predefinidos para usar.

Perfiles de ataques	Diseñado para proteger de
Default Detection	Todos los ataques.
Default DoS and Reconnaissance Only	Todas las firmas están deshabilitadas por defecto. Esta política se utiliza para el escenario donde una parte del tráfico debe de ser ignorado por el IPS.
Default Exclude Informational	Todos los ataques, incluyendo aquellos con firmas conocidas, pero omitiendo ataques de severidad informativa.
Default Prevention	Todos los ataques recomendados por el fabricante McAfee.
Default Testing	Similar al anterior, con la excepción de que las alertas de nivel informativo también son incluidas.
DMZ	Todos los tipos de ataques excepto aquellos *exploits* que utilizan TFTP, Telnet, RIP, NETBIOS, NFS y WINS.
DNS Server	Todos los ataques de reconocimiento y DoS, puertas traseras genéricas y *exploits* utilizando el protocolo DNS.
File Server	Todos los ataques de reconocimiento y DoS, puertas traseras genéricas y *exploits* utilizando protocolos DNS, NFS/RPC y NETBIOS/SMB
Inside Firewall	Todos los tipos de ataques excepto para aquellos *exploits* utilizando los protocolos TFTP, Tenet y RIP.
Internal segment	Todos los ataques excepto para exploits que utilizan RIP y protocolos de enrutamiento.
Linux Server	Todos los ataques donde el sistema operativo objetivo es Linux.
Mail Server	Todos los ataques de reconocimiento y DoS, puertas traseras genéricas y *exploits* utilizando los protocolos DNS; SMTP, POP3 e IMAP.
Outside Firewall	Todos los ataques excepto la categoría de reconocimiento (*Reconnaissance*).
Solaris Server	Todos los ataques donde el sistema operativo objetivo es Solaris.

Tabla 3. Lista de perfiles de ataque

5.14.2 POLÍTICAS ACTIVADAS POR DEFECTO EN EL PRODUCTO

101. Igualmente, el producto cuenta con varias políticas predeterminadas por defecto que sirven como punto de inicio en la *hardening* de la red:

Política	Diseñada para proteger contra
Default Prevention	Todos los ataques de gravedad baja o superior, con una acción de bloqueo por parte del sensor para todos los ataques de *McAfee Recommended for Blocking (RFB).*
Default Detection	Todos los ataques de gravedad baja o superior.
Outside Firewall	Todos los ataques menos los clasificados dentro de la categoría de reconocimiento.
DMZ	Todos los ataques menos los *exploits* usando TFTP, Telnet, RIP, NETBIOS, NFS y WINS.
Inside Firewall	Todos los ataques menos los *exploits* usando TFTP, Telnet y RIP.
Internal Segment	Todos los ataques menos los *exploits* usando RIP y protocolos de enrutamiento.
Web Server	Todos los ataques de reconocimiento y ataques DoS, *backdoors* comunes y *exploits* usando DNS, HTTP y FTP.
Mail Server	Todos los ataques de reconocimiento y DoS, además de exploits usando DNS, SMTP, POP3 e IMAP.
DNS Server	Todos los ataques de reconocimiento y DoS, *backdoors* comunes y *exploits* usando DNS.
File Server	Todos los ataques DoS y de reconocimiento, además de *backdoores* comunes y *exploits* usando SNS, NFS/RPC y NETBIOS/SMB.
Windows Server	Todos los ataques que pueden comprometer un sistema Windows.
Solaris Server	Todos los ataques que pueden comprometer un sistema Solaris.
UNIX Server	Todos los ataques que pueden comprometer un sistema Unix.
Linux Server	Todos los ataques que pueden comprometer un sistema Linux.

Política	Diseñada para proteger contra
Windows and UNIX Server	Todos los ataques que pueden comprometer un sistema Windows o UNIX.
Windows and Solaris Server	Todos los ataques que pueden comprometer un sistema Windows o Solaris.
Windows, Linux and Solaris Server	Todos los ataques que pueden comprometer un sistema Windows, Linux o Solaris.
Default Exclude Informational	Todos los ataques, incluyendo aquellos con firmas dudosas. Esta política difiere de la política *Default* en que alerta de cada ataque en la base de datos del NSP, pero sin crear alertas de información de la severidad del ataque.
Default Testing	Similar a *Default Exclude Informational*, pero incluyendo alertas sobre la severidad del ataque.
Default DoS and Reconnaissance Only	Todas las firmas están deshabilitadas por defecto. Esta política prevé un escenario donde un subflujo de tráfico necesita ser ignorado por el IPS.

Tabla 4. Lista de políticas por defecto para el hardening.

5.14.3 PREVENCIÓN CONTRA ATAQUES DOS

102. McAfee NSP dispone de una solución integrada de *hardware* y *software* para evitar ataques DoS y DDoS del orden de velocidad de varios GBs. La arquitectura NSP hace uso de una combinación auto aprendizaje, detección basada en perfiles y técnicas *threshold-based* para detectar ataques DoS/DDoS.

103. Con las técnicas *threshold-based* se puede configurar el límite de tráfico para asegurar que los servidores no se inutilicen debido a la sobrecarga. Por su parte, las metodologías de auto aprendizaje permiten al NSP estudiar los patrones y el uso medio de la red en un periodo de tiempo, aprendiendo y usando el conocimiento adquirido para mejorar en la detección de ataques DoS.

104. Las alertas de detección de ataques DoS se producen cuando un sensor detecta un tráfico anormal, una vulnerabilidad que pueda estar relacionada con un ataque DoS o ataques efectuados con herramientas de DoS. Para bloquear el tráfico DoS automáticamente es necesario configurar políticas de seguridad como se ha visto en puntos anteriores, aplicando un bloqueo del tráfico cuando un sensor detecte la anomalía.

5.14.4 PREVENCIÓN DE *MALWARE*

105. Una política de *malware* define un número de reglas para analizar el tráfico que circula por la red y determina cómo responder ante la detección de *malware*. En general, cuando un usuario descarga un archivo, tanto de forma íntegra, como de forma segmentada, el NSP a través de los sensores lo analiza y lo descarta si detecta malware.

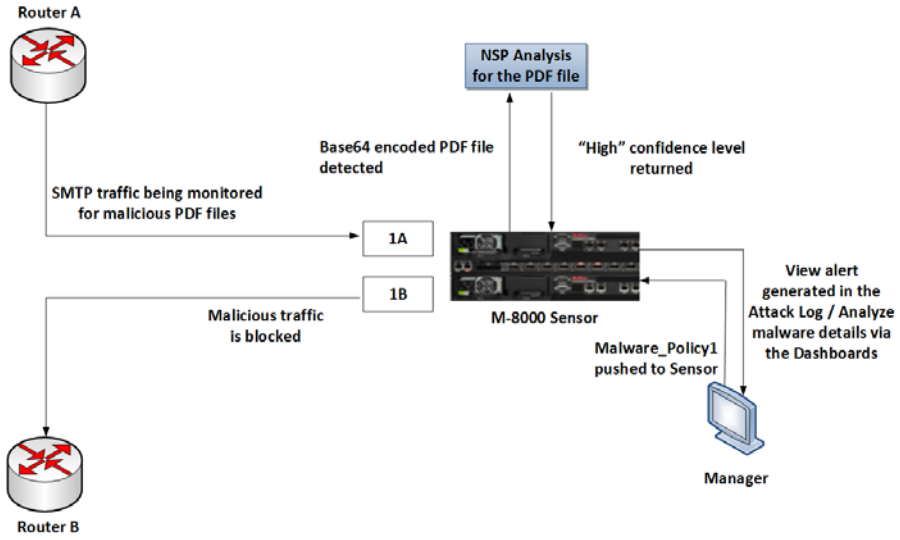

Ilustración 24. Detección avanzada de Malware usando Análisis NSP

106. Se recomienda crear políticas *anti-malware* diversas y específicas que se centren en las necesidades del negocio y en zonas de interés de la red. No se recomienda aplicar políticas generales de detección de *malware* a toda la red.

107. A continuación, se listan los módulos del sistema de prevención de *malware*:

a) ***TIE / GTI File Reputation***: usa el servicio en la nube McAfee *GTI File Reputation*, y el repositorio empresarial TIE (*Threat Intelligence Exchange*) para el análisis de archivos.

b) ***NSP Analysis***: es el encargado de analizar el código de ficheros tal como *JavaScript* en ficheros PDF o código *shell* en archivos *Flash* y archivos de Microsoft Office.

c) ***Gateway Anti-Malware Engine***: se encarga del bloqueo de amenazas *malware tales como gusanos, spyware o ramsonware.*

d) ***Advanced Threat Defense***: provee de protección contra malware novedoso y zero-day malware.

e) ***McAfee Cloud:*** se encarga del análisis de aplicaciones Android (APK), informando al administrador si se detecta *malware*.

6 FASE DE OPERACIÓN

108. Una vez el producto está configurado de forma segura y se encuentra en modo de funcionamiento normal, el usuario administrador responsable del dominio es el encargado de llevar a cabo las siguientes tareas de mantenimiento:

a) Administrar la base de datos del *Network Security Manager*, archivando y administrando la base de datos de alertas y registros generados por los sensores.

b) Organizar el plan de almacenamiento de la base de datos, haciendo hincapié en el plan de mantenimiento que tiene como objetivo mantener el rendimiento de la base de datos en un nivel óptimo. Esto se consigue eliminando archivos antiguos, alertas sin valor, registros y otros archivos tales como *back-ups* e informes que no sean requeridos.

c) Realizar *back-ups* periódicos y la restauración de estos. Además de almacenarlos en localizaciones seguras y planificar el proceso de automatización.

d) Actualizar periódicamente el *software* de los equipos, para garantizar que están al día, tanto en las capacidades de reconocimiento de aplicaciones, como en la prevención de amenazas.

e) Comprobar periódicamente el *hardware* y *software* para asegurar que no se ha introducido *hardware* o *software* no autorizado. El *firmware* activo y su integridad deberán verificarse periódicamente para comprobar que está libre de *software* malicioso.

f) Política de almacenamiento de archivos malware. El Manager permite la creación de una localización para almacenar todos los archivos descargados dependiendo de sus características. Estos archivos están cifrados en el *Manager Server*.

7 CHECKLIST

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto	☐	☐	
Consideraciones previas	☐	☐	
Registro de las licencias	☐	☐	
Instalación segura	☐	☐	
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
Modo de Operación seguro activado	☐	☐	
Elegir mecanismo de autenticación.	☐	☐	
Configuración de administradores	☐	☐	
Configuración de interfaces puertos y servicios	☐	☐	
Configuración de protocolos seguros	☐	☐	
Gestión de certificados	☐	☐	
Asignar servidor de autenticación (si es necesario)	☐	☐	
Sincronización horaria (servidor NTP)	☐	☐	
Configuración de actualizaciones automáticas	☐	☐	
Configuración protocolo SNMP	☐	☐	
Configurar Alta Disponibilidad	☐	☐	
Auditoría. Almacenamiento remoto (si aplica)	☐	☐	
Servicios de seguridad.	☐	☐	

Tabla 5. *Checklist* del procedimiento de empleo seguro

8 REFERENCIAS

REF1 *Mcafee Network Security Platform 9.1.X Product Guide*

REF2 *Mcafee Network Security Platform 9.1.X Certification Reference Guide*

REF3 *Mcafee Network Security Platform 9.1 (Manager Administration Guide)*

REF4 *Mcafee Network Security Platform 9.1 (IPS Administration Guide)*

REF5 *Mcafee Network Security Platform 9.1.X Installation Guide*

9 ABREVIATURAS

ACL	Lista de control de acceso
AES	*Advanced Encryption Standard*
API	Interfaz de programación de aplicaciones
CA	Autoridad de certificación
CHAP	*Challenge Handshake Authentication Protocol*
CLI	Interfaz de línea de comandos
CPD	Centro de Proceso de Datos
CSR	*Certificate Signing Request*
DDoS	Denegación distribuida de servicio
DHCP	Protocolo de configuración dinámica de host
DNS	Sistema de nombres de dominio
DoS	Denegación de servicio
ENS	Esquema Nacional de Seguridad
FIPS	*Federal Information Processing Standard*
FQDN	*Fully Qualified Domain Name*
HTTP	Protocolo de transferencia de hipertexto
IDPS	Sistema de detección y prevención de intrusiones
IMAP	Internet Message Access *Protocol*
IP	Protocolo de Internet / Dirección IP
IPS	Sistema de prevención de intrusiones
LDAP	Protocolo ligero de acceso a directorios
MAC	Media Access Control
MD5	*Message-Digest Algorithm 5*
MDR	*Manager Disaster Recovery*
MLOS	McAfee Linux Operating System
NFS	Sistema de archivos de red
NS	*Network Sensor*
NSM	*Network Security Manager*
NSP	*Network Security Platform*
NTBA	*Network Threat Behavior Analysis*
NTP	*Network Time Protocol*
OVF	Open Virtualization Format
PAP	*Password Authentication Protocol*
POP3	Protocolo de Oficina de Correo
QoS	Calidad del servicio
RADIUS	Remote Authentication Dial In User Service
RDBMS	*Relational DataBase Management System*
RIP	*Routing Information Protocol*
RPC	Llamada a procedimiento remoto
SHA	Algoritmo de Hash Seguro

SMB	*Server Message Block*
SMTP	Protocolo para transferencia simple de correo
SNMP	Protocolo simple de administración de red
SSH	Secure Shell
SSL	Seguridad de la capa de transporte
TACACS+	Terminal *Access Controller Access Control System plus*
TCP	Protocolo de control de transmisión
TFTP	Protocolo de transferencia de archivos trivial
TIE	*Threat Intelligence Exchange*
TLS	Seguridad de la capa de transporte
TOE	*Target of Evaluation*
UDP	Protocolo de datagramas de usuario
URL	Localizador de recursos uniforme

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL