centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1415

Procedimiento de Empleo Seguro
UTM/NG-*Firewall* de *Stormshield*

Junio 2020

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

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
2020.06.09 17:44:18 +02'00'

NIPO: 083-20-129-4.

Fecha de Edición: junio de 2020

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

PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

Junio de 2020

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

1 INTRODUCCIÓN

1. El UTM/NG-*Firewall* de *Stormshield* es un dispositivo que proporciona funciones de seguridad para permitir la interconexión entre una o varias redes de confianza a través de redes no controladas.

2. Concretamente, para un entorno similar al mostrado en **Figura 1**, aporta dos (2) grandes grupos de funcionalidades de seguridad:

   - La primera es la de actuar como cortafuegos de nueva generación, de forma que el UTM/NG-*Firewall* de *Stormshield* se sitúe como delimitación de las redes de confianza y la red no controlada para proteger las estaciones de trabajo y los servidores de la organización del tráfico proveniente de la red no controlada y llevando a cabo las siguientes tareas: filtrado y control de flujo de la información, detección de ataques, administración del ancho de banda, administración de políticas de seguridad, auditoría y autenticación de los administradores.

   - Uso de túneles VPN (*Virtual Private Network*) implementando ESP (*Encapsulating Security Payload*) en la zona no controlada de la red para proporcionar confidencialidad, autenticación en integridad sobre túneles IPSec securizando la transmisión de información a través de la red no controlada entre un cortafuegos de *Stormshield* y una estación de trabajo con un cliente VPN o bien entre dos cortafuegos de *Stormshield*.

3. Adicionalmente, implementa la tecnología ASQ (*Active Security Qualification*) para la prevención de intrusiones en tiempo real, basada en el análisis multicapa para prevenir la mayoría de ataques sin afectar al comportamiento del dispositivo y reduciendo al mismo tiempo el número de falsos positivos. Esta tecnología se basa en un sistema de avisos y alarmas que es totalmente configurable.

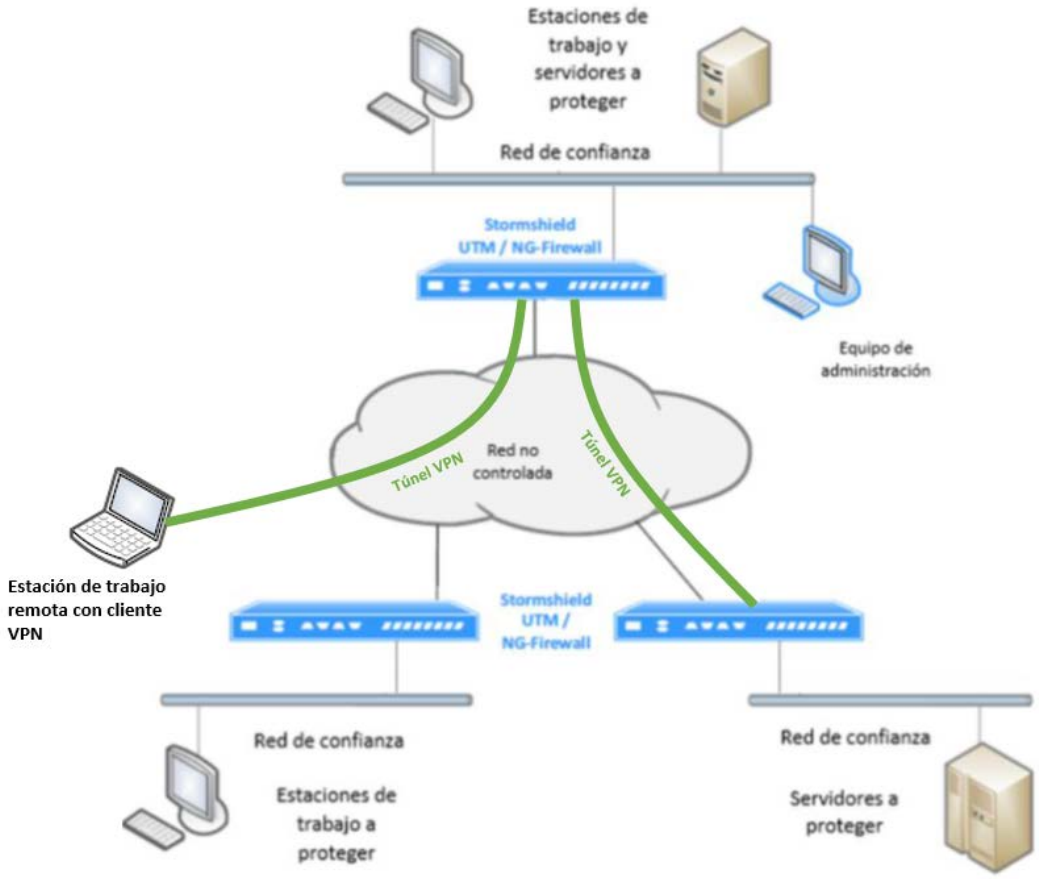

Figura 1: Entorno de operación.

1.1 CONTROL DE FLUJO

4. El cortafuegos de *Stormshield* permite definir una política de seguridad para determinar qué entidades (usuarios o dispositivos IT) pueden establecer flujos de información con otras entidades. Concretamente, el cortafuegos permite las siguientes funcionalidades de filtrado:

    a) Filtrado de flujo de información entre dispositivos basado en el protocolo, dirección IP de fuente y destino y los puertos TCP y UDP de fuente y destino, la fecha y la identidad del usuario autenticado de forma satisfactoria.

    b) Generación de auditoría para analizar las interconexiones y flujos de datos entre entidades.

5. Adicionalmente, también permite definir las políticas de cifrado haciendo uso de protocolos y algoritmos como IPSec para proteger los flujos de información que contengan datos sensibles que deban ser protegidos. El uso de VPN sobre IPSec

para el cifrados de las comunicaciones proporciona las siguientes funcionalidades de seguridad:

a) Confidencialidad del flujo de información.

b) Anonimato de los equipos que están compartiendo información.

c) Integridad del tráfico de información mediante el uso de las siguientes medidas: integridad de paquetes, protección contra replicación y autenticación del emisor del paquete.

d) Autenticación mutua de los extremos del túnel VPN.

6. Todas estas medidas de control de flujo, se pueden complementar mediante el establecimiento de alarmas que el administrador del sistema puede definir para los eventos de seguridad que se desean detectar y que están relacionados con el filtrado y cifrado de las comunicaciones, así como con la tecnología ASQ.

1.2 PROTECCIÓN CONTRA ATAQUES EXTERNOS

7. La monitorización de los flujos de información entre las redes de confianza y la red no controlada hace posible denegar intentos ilícitos de comunicación estableciendo políticas de control de flujo. Puesto que los intentos de intercambio de información se registran en el log para poder ser auditados posteriormente, el cortafuegos cuenta con la capacidad de bloquear directamente los flujos de información para que en caso de intentos de inundación no se produzca una saturación del log de auditoría.

8. No obstante, a pesar del establecimiento de políticas para el control de flujo de información en función de las especificaciones de la red y de la organización, aún existen posibles vectores de ataque para un atacante con acceso a la parte no controlada de la red:

a) *Bypass* de la política de control de flujo establecida en el cortafuegos.

b) Ataque a los dispositivos de la red de confianza de la organización haciendo uso de las vulnerabilidades conocidas para los protocolos utilizados (IP, TCP, UDP, protocolos de aplicación, etc).

9. Para reducir el impacto de estos posibles ataques el cortafuegos hace uso de la tecnología ASQ para la prevención de intrusiones, ya que es capaz de llevar a cabo escaneos dinámicos a nivel de IP, de transporte y de aplicación. En la sección “5.14.4 PREVENCIÓN DE ATAQUES” se recoge una descripción de los posibles ataques detectados mediante esta tecnología.

1.3 RIESGO DE USO INAPROPIADO

10. La definición de una política de seguridad, es por lo general una tarea complicada que requiere competencias específicas y que presenta riesgo de error.

11. El mayor riesgo es el de llevar a cabo una mala definición de las políticas de filtrado, debido a que esto puede implicar grandes posibilidades de ataque. Por ello, el cortafuegos de *Stormshield* permite realizar separación de roles, de forma que solo las personas cualificadas puedan acceder a dicha funcionalidad, estableciendo para ello control de acceso para las funciones de administración de seguridad. Solo el usuario "*super administrador*" podrá conectarse por consola local.

12. Además, para mitigar los posibles problemas inherentes a dicho riesgo de uso inapropiado, el cortafuegos cuenta con funciones de copia de seguridad y restauración.

1.4 ENTORNO SEGURO

13. Suponiendo que las políticas de seguridad se implementan de forma adecuada, la única solución para poder llevar a cabo un ataque es la de modificar el comportamiento del cortafuegos. Esto se puede realizar de varias formas:

    a) Consiguiendo deshabilitar alguna funcionalidad de seguridad o modificando su configuración haciendo uso de un ataque local o remoto que permita hacer *bypass* de las funciones de seguridad.

    b) Obteniendo las credenciales de administrador.

14. Para contrarrestar la posibilidad de que las funciones de seguridad sean deshabilitadas o de que las credenciales de administrador puedan ser obtenidas, se deben tomar medidas para la seguridad física y lógica del cortafuegos. Por otro lado, la monitorización del acceso a las operaciones administrativas mencionadas anteriormente, se apoya en el uso de mecanismos de autenticación basados en autenticación mutua mediante certificado X.509 (TSL) o autenticación mediante usuario/contraseña (TLS).

15. Además, como la administración remota es posible llevarla a cabo desde una red no controlada, el cortafuegos de Stormshield cuenta con una función para proteger la confidencialidad e integridad de las sesiones de administración basadas en operaciones de cifrado.

2 OBJETO Y ALCANCE

16. La presente guía, recoge el procedimiento de empleo seguro de los cortafuegos de nueva generación de *Stormshield* con compilaciones S, M, L y XL (desde la serie SN160 a la SN6100) y con versión del firmware 3.10.1 que ofrecen funcionalidades IPS y VPN.

3 ORGANIZACIÓN DEL DOCUMENTO

17. El presente documento se estructura en las secciones indicadas a continuación, las cuales engloban el ciclo de vida completo del dispositivo, desde su recepción e instalación, así como hasta las tareas necesarias para su mantenimiento seguro tras la instalación del mismo:

    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 recoge una *checklist* que contiene todas las recomendaciones sobre la configuración relativas al cortafuegos de *Stormshield.*

4 FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

18. En la presente sección se detalla la lista de pasos necesarios para poder asegurar que el producto no ha sido manipulado afectando a su integridad durante el proceso de entrega al cliente:

    a) Información del envío. Tras la compra, debe comprobarse la documentación del envío para verificar que concuerda con la orden de compra, así como que el envío ha sido realizado por *Stormshield*.

    b) Embalaje externo. Deberá inspeccionarse el embalaje y el sello de calidad de *Stormshield* (mostrado en la Figura 2). Se debe verificar que el sello de calidad no ha sido cortado o deteriorado y que la caja no presenta daños que hayan permitido tener acceso al dispositivo o parte de él.

Figura 2: Sello de calidad de Stormshield

    c) Etiquetas de identificación. El cortafuegos contiene una etiqueta que muestra toda información relativa al producto (la referencia, el número de serie, la versión del *firmware*, etc). Se debe inspeccionar dicha etiqueta para verificar que la versión del producto es la versión cualificada.

Figura 3: Etiqueta de información de producto.

- Sello de garantía. Se deberá comprobar que el sello de garantía del dispositivo está intacto para verificar que el dispositivo no se ha abierto ni se ha manipulado. En caso de rotura o deterioro de dicho sello se anulará la garantía del producto.

Figura 4: Sello de garantía

19. En caso de identificarse algún problema durante la inspección del embalaje y el producto tras su recepción por parte del cliente, se deberá contactar con *Stormshield* indicando el número de pedido y una descripción del producto.
20. Dependiendo del modelo concreto, el producto se entrega con:
    a) Un cable de alimentación.
    b) Un adaptador de corriente.
    c) Un cable RJ45.
    d) Un cable serie DB9F.
    e) Un conjunto de patas de goma anti deslizantes.
    f) Tres antenas Wi-Fi enroscables.
    g) Un kit de instalación en rack.
21. Adicionalmente, el producto se envía con la siguiente documentación:
    a) Condiciones generales de uso y licencia de usuario.
    b) Reglas de seguridad y precauciones de instalación.

c) Guía de instalación rápida.

d) Guía para la instalación del producto en rieles (dependiendo del producto).

4.2 ENTORNO DE INSTALACIÓN SEGURO

22. El dispositivo deberá instalarse en un lugar que cuente con control de acceso, así como de medidas de seguridad relativas a los procesos que afectan al entorno de operación (uso de cables trenzados con cobertura metálica, cables etiquetados, etc), de forma que, solo se tenga acceso al cortafuegos bajo la supervisión del *super administrador*.

23. En caso de instalar el dispositivo sin hacer uso de un rack, se debe instalar equipado con sus patas de goma antideslizantes para reducir la posibilidad de que el aparato resbale de la superficie donde se ha instalado.

24. Para más información al respecto, consultar la sección "*Safety Rules*" de la guía de instalación del producto **[INSTALLATION-GUIDE].**

4.3 REGISTRO Y LICENCIAS

25. Se deberá registrar el producto (usando la clave de registro y el número de serie indicados en la etiqueta del producto) para acceder a las diferentes compilaciones del *firmware*, soporte técnico, etc. Para registrar el producto, es necesario dirigirse a la siguiente URL (*https://mystormshield.eu*). Se recomienda que esta actividad se realice siempre con la misma cuenta de usuario para poder llevar a cabo las gestiones relativas a caducidad y renovaciones de los servicios asociados a cada dispositivo de manera centralizada.

4.4 CONSIDERACIONES PREVIAS

26. Como consideraciones previas a la instalación del producto, es necesario disponer de:

    a) Versiones recientes de Microsoft Edge, Google Chrome o Mozilla Firefox, ya que a la interfaz de configuración del cortafuegos se accede desde el navegador web para poder llevar a cabo tanto la configuración como la monitorización una vez el dispositivo está configurado.

27. Adicionalmente, es necesario consultar las instrucciones de seguridad previas a la instalación en el siguiente documento **[SAFETY-RULES-SNRANGE]**

4.5 INSTALACIÓN

28. En esta sección se detallan los pasos a seguir para llevar a cabo la instalación del cortafuegos de forma segura, una vez situado sobre una superficie plana usando las patas de goma o montado sobre un *rack*:

a) Llevar a cabo la correcta interconexión del cortafuegos como se detalla a continuación:

- Enchufarlo a la toma de corriente.
- Conectar los puertos de red como se describe a continuación:
  - Interfaz 2 (entrada): Esta es la interfaz interna que debe conectarse a la estación de trabajo cliente.
  - Interfaz 1 (salida): Esta es la interfaz que proporciona al dispositivo acceso a internet.

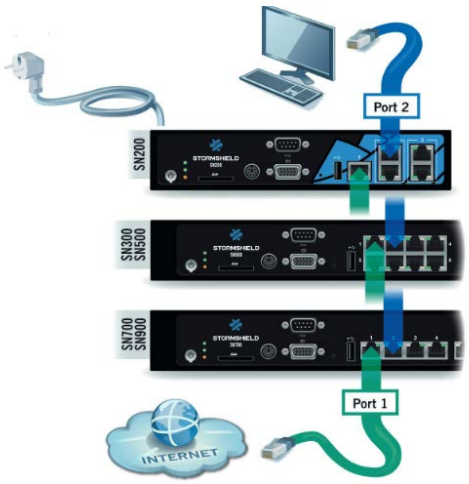

Figura 5: Conexión adecuada de los puertos de red.

b) Inicialización

- Presionar el botón de encendido una vez y esperar varios minutos hasta que los 3 *leds* (*Online, status* y *power*) se enciendan.

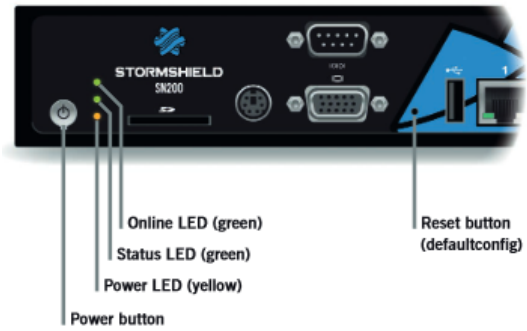

Figura 6: Identificación de los indicadores led del dispositivo.

- En la estación de trabajo cliente, acceder a la siguiente dirección en el navegador: *https://10.0.0.254/install*.
- Introducir las credenciales de super administrador cuyo valor es "*admin*" tanto para el usuario como para la contraseña. Estas credenciales deberán modificarse de acuerdo a la política de contraseñas establecida, tal como se describe en la sección 5.3.2.2 CONFIGURACIÓN DE LA POLÍTICA DE CONTRASEÑA.
- Un asistente de instalación guiará al usuario a través de la configuración del cortafuegos. El paso de registro permitirá al usuario acceder a su zona segura. El dispositivo debe registrarse para activar la garantía.
- Una vez se complete la instalación, se podrá acceder a la interfaz de configuración gráfica en la dirección *https://10.0.0.254/admin* para poder llevar a cabo la configuración segura del cortafuegos.

5 FASE DE CONFIGURACIÓN

5.1 MODO DE OPERACIÓN SEGURO

29. Para llevar a cabo la configuración segura del producto es necesario seguir los pasos detallados en las siguientes secciones.

5.2 AUTENTICACIÓN

5.2.1 AUTENTICACIÓN LOCAL DE USUARIOS

30. El cortafuegos de *Stormshield* ofrece la posibilidad de crear un directorio interno *menú "Users →Directories configuration"* que permite la autenticación local. Esta autenticación se usa para la conexión con servidores web y NSRPC (*NetAsq Secure Remote Protocol Client*). En este caso, el cortafuegos es el encargado de almacenar cualquier contraseña y sus derivados. También es posible autenticarse por medio del uso de un certificado.

31. En caso de establecer autenticación mediante certificado se deben seguir las indicaciones de la sección "5.6 GESTIÓN DE CERTIFICADOS".

32. Por otra parte, en caso de que un administrador necesite acceso al servidor NSRPC, que solo soporta acceso mediante contraseña, el establecimiento de la política de contraseñas se realizará accediendo a *"System → Configuration →General Configuration"* y siguiendo las recomendaciones de la guía [**DAT-NT-011**].

33. Adicionalmente, es posible configurar la autenticación mediante SSH para la cuenta de *super administrador* accediendo al menú "*System → Configuration → Firewall Administration*" y habilitando la opción *"Enable SSH Access".* Se recomienda no habilitar el acceso por contraseña para hacer uso de la autenticación mediante certificado.

5.2.2 AUTENTICACIÓN ENTRE COMPONENTES

34. Para evitar cualquier usurpación, independientemente del tipo de túnel configurado (sitio a sitio o cliente a sitio), es necesario autenticar al extremo remoto al crear el túnel. Es posible llevar a cabo la autenticación mediante el protocolo IKEv2 haciendo uso de un certificado.

35. Para implementar la autenticación mutua mediante certificado es necesario ir al menú "*VPN → IPSec VPN → Identification*" y seguir las indicaciones de la sección "5.14.2 VPN".

5.2.3 AUTENTICACIÓN CENTRALIZADA

36. El cortafuegos permite usar un sistema de autenticación centralizada basada en el uso de un directorio externo LDAP para limitar los datos almacenados de forma local, así como poder simplificar los procedimientos de administración.

37. **Por seguridad se recomienda el uso de un directorio LDAP externo.**

38. Cuando se hace uso de un directorio LDAP externo, se debe garantizar la confidencialidad y la integridad del flujo de información intercambiada durante la autenticación del equipo (cortafuegos y servidor de directorio), para evitar que un atacante pueda obtener información de la conexión.

39. Para configurar el directorio LDAP de forma segura, se recomienda:

    a) Hacer uso del protocolo LDAPS.

    b) Instalar un certificado generado por una PKI (*Public Key Infrastructure*) en el servidor LDAP.

    c) Importar la AC (Autoridad de Certificación) correspondiente.

    d) Usar la AC importada para validar la conexión al servidor LDAP.

40. La implementación de la autenticación desde un directorio externo se lleva a cabo en varios pasos:

    a) Activar el uso del directorio dirigiéndose al menú (*Configuration* → *Users* → *Directories configuration*), eligiendo el tipo de directorio y configurando el acceso:

        - Dirección del directorio.
        - Base DN.
        - Puerto de comunicación.
        - Identificador y contraseña para la cuenta de acceso al cortafuegos en el directorio. Es necesario considerar que la cuenta que el cortafuegos utiliza para acceder al directorio LDAP, debe quedar restringida únicamente para dicho uso. Particularmente, solo debe tener derechos de lectura para evitar cualquier modificación de los datos del directorio por parte del cortafuegos.

    b) En la pestaña "*Struture*" definir la estructura del directorio. Para ello, se debe establecer la correspondencia entre los atributos manejados por el cortafuegos y los presentes en el directorio LDAP. El atributo del miembro de *Stormshield* (que contiene la lista de identificadores pertenecientes a un grupo) debe en particular, corresponder a su equivalente en el directorio LDAP.

c) Definir LDAP como el método de autenticación predeterminado a través del menú "*Configuration* → *Users* → *Authentication*.

41. Para obtener información adicional acerca de la configuración del directorio LDAP externo se debe consultar la sección "*Connecting to an external LDAP directory*" del documento **[USER-CONFIG-MANUAL]**.

5.3 ADMINISTRACIÓN DEL PRODUCTO

5.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

42. Los usuarios administradores pueden llevar a cabo la administración del producto mediante la interfaz gráfica de administración accediendo a la siguiente URL (*https://10.0.0.254/admin*).

43. Adicionalmente los administradores pueden ejecutar comandos y llevar a cabo tareas de administración a través de la consola CLI (*Command Line Interface*). Para acceder a la misma es necesario ir al menú "*System* → *CLI*". Es posible consultar los comandos disponibles para la misma en la guía **[CLI-SERVERD-COMMAND]**.

44. Por otro lado, solo los usuarios *super administradores*, pueden llevar a cabo la administración remota del producto a través de SSH haciendo uso de comandos CLI. Los comandos disponibles, se puede consultar la guía **[CLI-CONSOLE/SSH-COMMAND].**

5.3.2 CONFIGURACIÓN DE ADMINISTRADORES

5.3.2.1 CREACIÓN DE USUARIOS ADMINISTRADORES

45. El cortafuegos de *Stormshield* permite definir dos (2) tipos de roles: el usuario *super administrador* y el usuario administrador.

46. Solo es posible definir un usuario *super administrador*, que será el único con permiso de acceso físico al cortafuegos, así como el encargado de supervisar cualquier tipo de acción sobre el mismo. Es el único con acceso a la consola local durante la instalación del cortafuegos o de llevar a cabo acciones de mantenimiento fuera de la operativa normal del producto.

47. Además, es el responsable de crear nuevos usuarios (administradores) y de asignar sus privilegios. Para crear nuevos usuarios administradores es necesario ir al menú "*System* → *Administrators*" y pulsar en el desplegable "*Add an administrator*" pudiendo elegir entre una de las siguientes opciones:

a) Administrador sin privilegios.

b) Administrador con privilegios solo de lectura.

c) Administrador con todos los privilegios.

d) Administrador con cuenta temporal.

e) Administrador con acceso a los datos privados.

f) Administrador sin acceso a los datos privados.

48. Es posible encontrar información adicional sobre cada tipo de usuario administrador en la sección "*Administrators*" del documento **[USER-CONFIG-MANUAL]**.

49. A la hora de definir administradores y privilegios asociados a estos deberá seguirse los principios de mínima funcionalidad y mínimo privilegio, de tal forma que se definan únicamente el número de administradores necesarios con los mínimos privilegios requeridos para realizar sus funciones.

5.3.2.2 CONFIGURACIÓN DE LA POLÍTICA DE CONTRASEÑA

50. El usuario *super administrador* puede configurar una política de contraseña desde la pestaña "*General configuration*" del menú *"System → Configuration*" para todas las contraseñas y claves pre compartidas que pueden ser usada en procesos de autenticación mediante VPN PPTP, IPSec, VPN, etc.

51. **La política de contraseña debe cumplir con las siguientes directrices y opciones de configuración:**

    a) Deberán ser de 12 caracteres como mínimo, aunque se recomienda una longitud de 15 caracteres. Para ello, ir al menú *"System →Configuration*" y fijar el parámetro "*Minimum password lenght"* al valor deseado.

    b) Deberán incluir caracteres alfanuméricos y caracteres especiales como "!", "@", "#", "$", "%", "^", "&", "*", "(" y ")", excepto espacio, tabulaciones o ("). Para ello, ir al menú *"System →Configuration*" y seleccionar en el desplegable asociado al parámetro "*Mandatory caracter types*" la opción *"Alphabetic and special".*

5.3.2.3 EL VALOR RECOMENDADO PARA LA VIGENCIA Y EXPIRACIÓN DE CONTRASEÑAS ES DE 30 DÍAS.CONFIGURACIÓN DE LOS PARÁMETROS DE SESIÓN

52. Es posible configurar el tiempo de inactividad de sesión para un usuario administrador a través de la interfaz gráfica de administración. Para ello es necesario ir a la sección "*Preferences*" situado en la parte superior derecha de la

pantalla y en la sección "*Connection settings*" se podrá establecer un valor de 5 minutos, 15 minutos, 30 minutos (valor por defecto) o 1 hora. **Se recomienda la configuración del menor tiempo de inactividad posible.**

53. El usuario administrador también podrá configurar el tiempo de inactividad de sesión para el acceso mediante SSH (por defecto 30 minutos) siguiendo los siguientes pasos:

    a) Editar el fichero *"/usr/Firewall/.login"* para modificar el parámetro de la primera línea llamado *"set autologout = XX"* donde "XX" es el *timeout* en minutos. **Se recomienda la configuración del menor tiempo posible que permita la correcta administración.**

    b) Copiar el fichero *"/usr/Firewall/.login"* en la carpeta *"/log*" haciendo uso del comando *"cp /usr/Firewall/.login /log/.login*. De esta forma se garantiza que la configuración se mantendrá ante posibles actualizaciones del firmware.

    c) Finalmente es necesario crear el fichero "*/etc/rc.user*" el cual se autoejecuta durante el arranque y poner el su interior el siguiente comando para que la configuración sea persistente ante posibles reinicios del cortafuegos:

    - *touch /etc/rc.user*
    - *echo "cp /log/.login /usr/Firewall/.login" > /etc/rc.user*

54. Para configurar el número máximo de intentos de autenticación, así como el tiempo de espera tras superar dicho umbral, es necesario ir al menú *"System → Configuration → Firewall administration"* y habilitar la protección contra ataques de fuerza bruta "*Enable protection from brute force attacks*", pudiendo configurar el número máximo de intentos de autenticación fallidos (por defecto es 3) y el tiempo de espera en minutos (siendo 60 minutos su valor máximo). **En cualquier caso, el número de intentos fallidos de autenticación no debería ser superior a 5 intentos.**

55. Por otro lado, el cortafuegos permite definir configurar el *banner* que será mostrado en el *login* de la interfaz gráfica de administración. Para ello es necesario ir al menú "*System → Configuration → Firewall administration*" y en la sección "*Disclaimer*" subir un archivo con extensión "*.txt*" que contenga el mensaje deseado para ser mostrado en el banner. **Se debe configurar un banner que informe a los usuarios que acceden al sistema que se podrán tomar las oportunas medidas en caso de acceso no autorizado.**

5.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

5.4.1 CONFIGURACIÓN DE RED

56. **Se deben deshabilitar todas las interfaces de red no utilizadas para disminuir la superficie de ataque.** El cortafuegos permite llevar a cabo dicha configuración de red accediendo para ello al menú "*Network → Interfaces*".

57. Por otro lado, como se verá en los siguientes apartados, el cortafuegos permite llevar a cabo la configuración de IP *anti-spoofing* para evitar posible suplantación de IP.

5.4.1.1 CONFIGURACIÓN DE IP *ANTI-SPOOFING*

5.4.1.1.1 PRINCIPIO DE IP ANTI-SPOOFING

58. La suplantación de IP consiste en simular una dirección IP legitima con el fin de eludir las normas de filtrado implementadas. Por ejemplo, se puede conseguir mediante el envío de paquetes desde la red externa originados en una dirección IP interna con destino otra dirección IP interna. Sin la verificación de las interfaces utilizadas, el cortafuegos interpreta la petición como legítima y procedente de la red interna y con destino la red interna, de forma que se consigue encaminar el tráfico malicioso como tráfico interno legítimo.

59. Los mecanismos de *anti-spoofing* están activos por defecto, verificando en cada interfaz de entrada la legitimad de la dirección IP de origen de los paquetes. Esa legitimidad se basa en la topología de red definida por:

    a) Interfaces de red para redes conectadas directamente.

    b) La tabla de enrutamiento para redes remotas.

60. El cortafuegos utiliza la noción de interfaz "interna" para identificar las interfaces que alimentan el mecanismo *anti-spoofing*. En el menú "*Network → Interfaces → Configuration of the interface*" se permite configurar el tipo de interfaz, apareciendo un escudo cuando la interfaz está protegida contra *anti-spoofing*. Por lo tanto, dicha interfaz solo aceptará paquetes cuya dirección IP de origen provenga de la red comunicación de la interfaz. Además, las otras interfaces no protegidas (sin escudo) del cortafuegos rechazarán esos mismos paquetes como entrada. Estas *reglas anti-spoofing* se aplican antes que la evaluación de la política de filtrado de red.

61. **Nota:** Las reglas de filtrado implícito permiten la administración de equipos desde interfaces internas, dichas reglas deben de ser desactivadas en el menú "*Security Policy → Implicit rules*"

62. La definición de rutas estáticas da información al cortafuegos acerca de la topología de red e implícitamente completa los mecanismos anti suplantación (*anti-spoofing*). Cualquier ruta a una red remota accesible por una interfaz interna se agrega a las tablas de *anti-spoofing*. Las rutas que utilizan interfaces externas no están protegidas porque, en general, se utilizan para responder a los equipos cuyas direcciones IP de origen no se conocen de antemano.

63. Se deben definir rutas estáticas para todas las redes internas conocidas a las que no pertenecen las interfaces de los cortafuegos, a fin de aprovechar los mecanismos *anti-spoofing*. Estas rutas se pueden reconocer en el *menú "Network → Interfaces"* por la presencia de un escudo.

64. **Nota:** Es necesario declarar rutas para todas las redes remotas accesibles por las redes internas. De lo contrario, sus paquetes serán rechazados sistemáticamente por el cortafuegos.

5.4.1.1.2 *ANTI-SPOOFING* EN UN PUENTE

65. Un puente permite conectar varias interfaces físicas en la misma red. El cortafuegos, sin embargo, aplica sus mecanismos *anti-spoofing* de forma independiente en cada una de las interfaces del puente.

66. Cuando los dispositivos están en la misma red de conmutación que el cortafuegos, este último mantiene una tabla que contiene cada dirección IP encontrada y la interfaz física asociada. Si se detecta una dirección en una interfaz diferente a la ingresada, entonces se produce una alerta.

67. La tabla de *host* se rellena cuando un dispositivo envía al menos un paquete. Por tanto, si el dispositivo no envía ni un solo paquete, no estará protegido contra *anti-spoofing on bridge*.

5.4.2 CONFIGURACIÓN DE SERVICIOS

68. El cortafuegos permite al *super administrador* poder llevar a cabo la configuración de los servicios proporcionados por el propio cortafuegos: el acceso al mismo mediante SSH (como se detalla en la sección "5.2.1 AUTENTICACIÓN LOCAL DE USUARIOS"), la autenticación haciendo uso de certificados como se detalla en la sección "5.6 GESTIÓN DE CERTIFICADOS" o los propios servicios a los que cada usuario administrador tendrá acceso.

69. Además, ciertos servicios serán de vital importancia para el correcto funcionamiento del dispositivo, como puede ser el servicio de actualización activa detallado en la sección "5.9.1 SERVICIO DE ACTUALIZACIÓN ACTIVA DE MÓDULOS"

o la configuración de DNS para dar soporte a otros servicios como puede ser *proxy web*.

5.4.2.1 DNS

70. Si los servidores DNS se ven comprometidos, un atacante podría redirigir los flujos de forma ilegítima. El cortafuegos permite crear objetos estáticos y dinámicos. En la configuración por defecto existen objetos con resolución dinámica que corresponden a servidores de actualización de firmas de Stormshield y que dependen de un nombre de host que el cortafuegos resuelve regularmente. Esto genera consultas DNS que podrían no ser deseables.

71. Para garantizar la seguridad de estas consultas regulares de DNS se recomienda modificar la configuración por defecto elegiendo servidores DNS de confianza en el menú *"System → Configuration → Network settings"*: se recomienda cambiar los servidores DNS predeterminados por aquellos del proveedor de acceso en caso que no exista ninguno que esté dentro del propio dominio del Sistema de Información.

72. Además, se recomienda eliminar los objetos dinámicos no usados y volver a configurar los objetos restantes en modo estático, accediendo al menú "*Objects → Network objects".*

5.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

73. El cortafuegos hace uso de protocolos de comunicaciones seguras en los siguientes casos:

    a. Administración a través de la web. Para lo cual utilizará canales TLS.

    b. Envío de auditoría a un servidor remoto mediante TLS.

    c. Establecimiento de VPN para la protección de la información en redes no controladas, para lo cual utiliza el protocolo IPSec o VPN SSL.

74. El cortafuegos está configurado por defecto para rechazar todas las conexiones a la web de administración que usen una versión inferior a TLS 1.2. Todas las sesiones entre la web de administración y el cortafuegos están cifradas haciendo uso de los siguientes algoritmos / mecanismos criptográficos:

    a. AES 128 o 256 bit para proporcionar confidencialidad de la información.

    b. HMAC-SHA2 con longitud de clave de 256 o 384 bits para proporcionar integridad a la comunicación.

    c. Certificados de tipo X.509 v3 para la autenticación mutua durante el establecimiento del canal TLS. La autenticación y el cifrado de las claves de

las sesiones de administración remota se derivan de la clave de sesión durante el establecimiento del canal TLS, ya sea con o sin autenticación mutua, mediante el uso de certificados de tipo X.509 v3.

75. La lista de *cipher suites* disponibles es la siguiente:

    - *ECDHE-RSA-AES128-GCM-SHA256*
    - *DHE-RSA-AES128-GCM-SHA256*
    - *ECDHE-RSA-AES128-SHA256*
    - *DHE-RSA-AES128-SHA256*
    - *ECDHE-RSA-AES256-GCM-SHA384*
    - *DHE-RSA-AES256-GCM-SHA384*
    - *ECDHE-RSA-AES256-SHA384*
    - *DHE-RSA-AES256-SHA256*

76. El cortafuegos cuenta con un comando del CLI para configurar las *ciphersuites* de cifrado a usar (en caso de querer añadir más *cipher suites* seguras). Para ello, es necesario acceder al menú "*System → CLI*" e introducir el siguiente comando:

    CONFIG AUTH HTTPS cipherlist="Lista de cipher suites separadas por comas" sslparanoiac=1. El parámetro *sslparanoiac* está configurado a 1 por defecto, implicando que se rechazarán todas las conexiones de clientes que usen una versión inferior a TLS 1.2.

77. Por otro lado, el cortafuegos provee la capacidad de asegurar el flujo de datos a través de redes no controladas haciendo uso de canales VPN. Suministra confidencialidad y autenticación haciendo uso del cifrado mediante IPsec con IKEv2. La información relativa a la correcta configuración de IPsec para hacer uso de IKEv2, así como para hacer uso de perfiles de cifrados recomendados, se encuentra en la sección "5.14.2 VPN".

5.6 GESTIÓN DE CERTIFICADOS

78. El cortafuegos permite el uso de certificados X.509v3 para los siguientes casos:

    - Publicación de la interfaz de administrador web haciendo uso de HTTPS.
    - Autenticación de certificado de administrador para acceso a la interfaz web de administración.
    - Autenticación de usuarios y puertas de enlace en el contexto de la configuración de túneles IPsec VPN.

- Autenticación de usuarios y puertas de enlace como parte de la implementación de un servicio SSL/TLS VPN.
- Conexión a un directorio externo LDAP.

5.6.1 USO DE UNA PKI

79. Cuando un equipo está involucrado en un mecanismo de autenticación, puede confiar en certificados de una PKI. La confianza depositada en la PKI determina la confianza del certificado utilizado, y, por tanto, la fiabilidad de la autenticación. En ausencia de una solución externa de gestión de certificados, el cortafuegos de *Stormshield* ofrece la posibilidad de generar una Autoridad de Certificación y los certificados firmados por ella. En este caso, las claves privadas son generadas y almacenadas por el cortafuegos de forma que en caso de que el cortafuegos sea comprometido, también lo serán las claves.

80. Se recomienda hacer uso de una PKI controlada de forma externa al cortafuegos para generar los certificados que utiliza. La PKI y la CA utilizadas deben cumplir con las recomendaciones de la **[RGS].**

81. En caso de no poder usar una PKI externa y generar el certificado de forma interna en el dispositivo, las claves generadas por este deberán eliminarse después de su exportación al equipo de destino. Además, en este caso, se recomienda que esta función se restrinja a ser usada en equipos con la menor exposición posible a redes no controladas. Para poder generar certificados de forma interna, es necesario primero que el super administrador genere una CA interna o bien, hacer uso de la CA preconfigurada cuyo CN está asociado al número de serie del dispositivo. El certificado de usuario vendrá firmado por dicha CA.

5.6.2 GESTIÓN DE CRL EN EL MARCO DE UN TÚNEL IPSEC

82. En caso de que un certificado sea revocado puede suceder que un usuario o equipo ilegítimo se beneficie de dicho certificado para autenticarse en el cortafuegos si este no ha sido notificado de que el certificado no es válido.

83. Para solucionar dicho problema, el cortafuegos permite llevar a cabo el establecimiento de CRL (*Certificate Revocation List*) por parte de la PKI para que el cortafuegos pueda verificar la revocación de certificados. Por defecto, si no cuenta con una CRL, entonces no impedirá el establecimiento de una VPN IPsec.

84. Por tanto, es necesario imponer la verificación de CRL para la implementación de túneles IPSec siguiendo los siguientes pasos:

    a) Acceder al CLI desde el menú "*System* → *CLI*".

b) Establecer el parámetro *CRLrequired* y reiniciar el servicio usando para ello, es necesario utilizar los siguientes comandos:

- *config ipsec update slot =01 CRLrequired =1*
- *config ipsec activate*

Nota: El slot=01, hace referencia al número del perfil de configuración de IPsec empleado. El cortafuegos cuenta con varios perfiles de configuración numerados del 01 al 10 y que pueden ser activados con el siguiente comando *"envpn 00 && envpn 01"* (en este ejemplo se desactiva la configuración VPN y a continuación se activa el perfil de configuración 01).

5.6.3 IMPORTACIÓN AUTOMÁTICA DE CRL

85. Una vez establecida la CRL, es importante también tener en cuenta la frecuencia de actualización de la misma para conocer qué certificados han sido revocados para evitar que se produzca la autenticación de certificados ya revocados. Aunque el periodo de actualización se debe establecer en base al tiempo más corto requerido por los diferentes servicios que hacen uso del certificado, un valor aceptable podría ser 6 horas.

86. Por defecto este valor es de 24 horas, y para modificarlo, es necesario agregar una nueva entrada en el archivo */ConfigFiles/Event/rules* haciendo uso del comando, donde 21600 es el valor en segundos de las 6 horas a configurar:

PKI CONFIG UPDATE checkcrlperiod=21600

87. Del mismo modo, se recomienda configurar la URL de recuperación automática de la CRL de cada CA activando la funcionalidad en el menú *"System → Configuration".*

88. Para fijar los puntos de distribución de CRL asociados a una CA, se pueden fijar a través de la web de administración en la pestaña CRL de la CA en cuestión o bien a través de la línea de comandos con el comando:

pki ca checkcrl add caname = <nombre de AC> uri = <URL de CRL>

Nota: La URL del punto de distribución puede ser HTTP, HTTPS, LDAP, LDAPS y FTP.

5.6.4 IMPORTACIÓN MANUAL DE CRL

89. Pueden surgir situaciones en las que no sea posible importar automáticamente una CRL. Para estos casos, el cortafuegos permite la importación de forma manual, lo cual implica, la intervención de un administrador y la manipulación de archivos, lo

cual, requiere procedimientos de organización estrictos, siendo una operación excepcional.

90. La importación manual de una CRL se realiza desde la web de administración a través del menú "*Objects → Certificates and PKI → Add → Import a file*". El archivo CRL debe ser importado en formato PEM o DER y su nombre no debe incluir extensión. También es posible copiar directamente el archivo CRL en formato PEM en el directorio de la CA, nombrándolo como CA.crl.pem.

5.7 SERVIDORES DE AUTENTICACIÓN

91. Como se ha indicado en la sección "*5.2.3* AUTENTICACIÓN CENTRALIZADA" del presente documento, el cortafuegos permite llevar a cabo la autenticación de forma centralizada haciendo uso de un servidor LDAP externo.

5.8 SINCRONIZACIÓN HORARIA

92. Varias características de seguridad del dispositivo como son la del registro y la gestión de certificados, están fuertemente ligadas a la hora del sistema, por tanto, es de vital importancia que el cortafuegos cuente con una fuente de tiempo de confianza.

93. Para ello, se recomienda activar la sincronización NTP del equipo especificando varios servidores de tiempo confiables a través del menú "*System → Configuration*" y en la pestaña "*General configuration*" habilitar la opción "*Synchronize firewall time (NTP)*" para poder añadir los servidores de confianza deseados.

94. Es posible disponer de información adicional relativa a la sincronización NTP en la sección "*Configuration*" del manual de usuario **[USER-CONFIG-MANUAL]**.

5.9 ACTUALIZACIONES

95. El dispositivo permite al *super administrador* poder habilitar/deshabilitar la búsqueda de actualizaciones automáticas para los módulos del mismo relacionados con filtrado de *URLs, antivirus, anti-spam*, etc. Para ello, es necesario dirigirse al menú "*Configuration → Active Update*" para habilitar o deshabilitar todas las actualizaciones o hacerlo de forma independiente para cada una de ellas.

96. Por otro lado, en cuanto a las actualizaciones del *firmware* del producto de forma segura, el dispositivo permite llevar a cabo la instalación de

actualizaciones de forma manual o automática una vez el cortafuegos haya verificado la firma de estas.

5.9.1 SERVICIO DE ACTUALIZACIÓN ACTIVA DE MÓDULOS

97. Las actualizaciones de los módulos se pueden llevar a cabo de dos formas distintas:

    a. En modo offline configurando un mirror interno.

    b. En modo online, a través de un proxy o de forma directa.

5.9.1.1 MIRROR INTERNO (MODO OFFLINE)

98. Para la actualización offline es necesaria la utilización de un *mirror* interno. Esto permite restringir la cantidad de dispositivos que se conectan a internet y es especialmente útil en entornos en los que se cuenta con varios cortafuegos *Stormshield* en la estructura de red, de forma que, si todos acceden a las actualizaciones a la vez a través de internet, puede causar un uso excesivo del ancho de banda.

99. Las actualizaciones no pueden ser desplegadas en los equipos sin utilizar un *mirror* interno. Sin embargo, las actualizaciones sí pueden ser descargadas de internet y desplegadas en el *mirror* de forma manual.

100. Se recomienda actualizar los servicios regularmente activando las actualizaciones automáticas y el uso de un espejo interno.

5.9.1.2 ACTUALIZACION DIRECTA (MODO ONLINE)

101. En este caso se recomienda que la conexión al servidor de actualización solo sea usada por el cortafuegos, lo que se puede conseguir configurando un servidor proxy de autenticación con una cuenta dedicada con acceso restringido a las necesidades del equipo y una política de filtro adecuada.

5.9.2 ACTUALIZACIÓN AUTOMÁTICA DE FIRMWARE

102. Para proceder con la actualización de manera automática a través del propio cortafuegos, es necesario ir al menú "*Configuration* → *System* → *Maintenance*" y hacer *clic* en "*Search for new updates*" para que el dispositivo consulte en el portal de *MyStormshield* si existen nuevas actualizaciones de software disponibles. En caso afirmativo, el cortafuegos mostrará al usuario la nueva versión disponible y verificará la firma de la misma antes de proceder con la instalación. La verificación de la firma se realiza por medio de claves RSA de 4096 bits de longitud.

5.9.3 ACTUALIZACIÓN MANUAL DE FIRMWARE

103. En este caso, es necesario que el *super administrador* acceda al portal *MyStormshield* para consultar si existen nuevas versiones del firmware. En caso afirmativo, será posible consultar en el portal el *hash* de tipo SHA2 del mismo.

104. Una vez descargada la nueva versión del *firmware*, accediendo al menú "*Configuration → System → Maintenance*", se seleccionará el archivo en la sección "*Select an update file*" y a continuación se hace *clic* sobre el botón "*Update firmware*".

105. Al igual que en el caso anterior, el dispositivo solo procederá a realizar la actualización una vez haya validado la firma, basada en el uso de RSA de 4096 bits de longitud.

5.10 SNMP

106. **Se debe configurar SNMPv3 frente a otras versiones anteriores menos seguras**. El cortafuegos permite hacer uso de dicha versión que proporciona mecanismos de autenticación y cifrado.

107. Para proceder con la correcta configuración del protocolo, en primer lugar, es necesario configurar los parámetros de ubicación (*syslocation*) y contacto (*syscontact*) de forma adecuada desde el menú "*Notifications → SNMP Agent → General*", para facilitar el mapeo de equipos en las herramientas de supervisión y alerta.

108. En segundo lugar, para habilitar el uso de SNMPv3, desde el mismo menú es necesario habilitar la opción "*Enable the Agent*" y activar el uso de SNMPv3, finalmente, en la pestaña "*SNMP V3*", se podrá configurar los parámetros necesarios para llevar a cabo la autenticación y el cifrado.

109. Es posible consultar información adicional relacionada al uso y configuración de SNMP en la sección "*SNMP Agent*" del documento **[USER-CONFIG-MANUAL].**

5.11 ALTA DISPONIBILIDAD

110. El cortafuegos de *Stormshield* permite crear un grupo o clúster de cortafuegos, para posteriormente añadir otro cortafuegos al clúster creado.

111. Los dispositivos que componen el clúster pueden funcionar de dos modos "activo/pasivo". El cortafuegos en modo activo, será el que normalmente se encuentre operando, mientras que, por el contrario, el pasivo será el que esté a la espera de entrar en funcionamiento en caso de que el primero falle.

112. La configuración de funcionamiento en modo alta disponibilidad consta de cuatro (4) pasos:

    a) Creación del clúster o bien unión al clúster: Durante este proceso, un cortafuegos se preparará para iniciar un nuevo clúster (al que se unirán otros cortafuegos) o bien para unirse a otro clúster, previamente inicializado por otro cortafuegos.

    b) Configurar las interfaces de red: Se debe configurar la interfaz de conexión entre ambos cortafuegos y opcionalmente un segundo interfaz de respaldo.

    c) Creación de la clave compartida: Será necesario crear una clave precompartida que se usará solamente cuando los cortafuegos se unen al clúster por primera vez. Dicha clave es utilizada para la autenticación de la conexión inicial entre los miembros del clúster, para permitir que un nuevo miembro se una al clúster por primera vez.

    d) Resumen y finalización: Durante esta fase se muestra un resumen de la configuración establecida y finalizar la misma.

113. Para tener más detalle acerca de la configuración del dispositivo en alta disponibilidad se puede consultar la información disponible en la sección "High Availability" del documento **[USER-CONFIG-MANUAL]** o bien visualizar el contenido del este video[1] facilitado por Stormshield.

5.12 AUDITORÍA

5.12.1 REGISTRO DE EVENTOS

114. Los registros de auditoría contienen eventos relacionados con administración del dispositivo, alarmas, autenticación, conexiones de red, filtrado de red, proxy FTP, IPSec VPN, conexiones de aplicación, proxy SMTP, proxy SSL, eventos de sistema, vulnerabilidades, proxy HTTP y SSL VPN.

115. Para cada uno de los eventos existe un fichero de log independiente, donde los eventos se registran según su tipo.

116. Aunque todos los ficheros de logs listados anteriormente contienen campos comunes, dependiendo del tipo de evento contendrá campos adicionales. El contenido específico de cada fichero de log se puede consultar en el documento **[AUDIT-LOG-TEC-NOTE].**

[1] https://www.youtube.com/watch?v=kd56VGZ76Og&hd=1

5.12.2 ALMACENAMIENTO LOCAL

117. El almacenamiento local máximo disponible para el almacenamiento de logs depende del modelo de cortafuegos (por ejemplo, eL producto SNS710 cuenta con 6GB). Cada cortafuegos permite configurar el espacio reservado para dichos registros, así como la capacidad para evitar que dicho espacio se agote en caso de intentos de inundación de red.

118. Para poder configurar el espacio reservado para dichos registros es necesario ir al menú *"Configuration → Logs-Syslog-IPFIX"* y asignar el tanto por ciento deseado para cada registro.

119. En caso de que se agote el espacio de almacenamiento reservado para los registros de auditoría, el producto permite al *super administrador* elegir entre borrar los registros más antiguos o pausar el registro de logs de auditoría. **Se recomienda que la configuración a aplicar, en caso de llenado del almacenamiento, sea la del borrado de los registros más antiguos.**

120. Es posible consultar información adicional al respecto en la sección "Logs-Syslog-IPFIX" del documento **[USER-CONFIG-MANUAL].**

5.12.3 ALMACENAMIENTO REMOTO

121. Como almacenamiento remoto o externo, el dispositivo ofrece la posibilidad (en modelos SN160, SN210, SN310) de hacer uso de una tarjeta de memoria SD de hasta 2TB, que debe ser de clase 10 y que cumpla con los estándares SDHC (*Secure Digital High Capacity*) y SDXC (*Secure Digital Extended Capacity*). El resto de modelos solo disponen de almacenaje local de *logs* en disco duro interno.

122. Por otra parte, también cuenta con la funcionalidad de *Syslog* pudiendo configurar hasta cuatro tipos de perfiles para el envío de registros de auditoría haciendo uso de un canal seguro basada en el uso de TLS. Para ello, accediendo al menú "*Configuration* → Logs-Syslog-IPFIX" y la pestaña "*Syslog"*, es posible establecer una configuración distinta para cada uno de los 4 perfiles existentes.

123. Para cada perfil será necesario configurar el servidor externo donde se enviará el registro de auditoría, el formato de este, y el protocolo de comunicaciones que se utilizará, que deberá ser TLS, con objeto de garantizar que el canal establecido es seguro. Para consultar información adicional acerca de la configuración es posible consultar el apartado "*Using TCP TLS by importing certificates generated by the SVC sever's PKI"* de la sección "*4.2.2 Configuring SNS from V3 upwards" del documento [SVC-ADMIN-GUIDE].*

5.13 BACKUP

124. Como servicio de *backup*, el dispositivo permite llevar a cabo una ejecución manual para crear un *backup* de su configuración, que podrá ser protegido mediante contraseña. También podrá configurar *backups* automáticos que se hagan de forma periódica en un entorno seguro.

125. **Se debe configurar la realización de backups automáticos de forma periódica**. Para ello, en la web de administración es necesario ir al menú "*Configuration → System → Maintenance"* y en la pestaña de "*Backup*" habilitar la *opción "Enable automatic backup"* e introducir los datos del servidor de respaldo estableciendo como protocolo de comunicación HTTPS. Del mismo modo, también será posible especificar la frecuencia con la que se realizará la copia de seguridad y una contraseña para llevar a cabo el cifrado de la misma. Esta contraseña deberá cumplir la política de contraseñas establecida por el *super administrador.*

126. Para obtener instrucciones detalladas acerca de cómo llevar a cabo la configuración del servicio automático de backups, se puede consultar el documento **[SNENTNO_AUTOBACKUP]**.

5.14 SERVICIOS DE SEGURIDAD

5.14.1 POLÍTICAS DE CORTAFUEGOS

127. La tecnología ASQ incluye un motor de filtrado de paquetes dinámico que permite aplicar de forma optimizada las políticas de filtrado del cortafuegos. La implementación de la función filtrado se basa en la comparación de atributos de cada paquete IP recibido contra cada regla establecida en el cortafuegos. Esta función de filtrado se aplica a todos los paquetes sin excepción según los siguientes criterios de filtrado:

    a) La interfaz de recepción y destino del paquete IP que está cubierto por la regla.

    b) La máquina originaria del flujo de información al que aplica la regla.

    c) La máquina de destino del flujo de información al que aplica la regla.

128. Los atributos de los paquetes IP contra los que se comparan estos cuatro criterios, se obtienen de los encabezados de las tramas Ethernet, IP, ICMP, UDP y TCP.

129. Cada regla de filtrado, establece una acción a realizar sobre el tráfico al que aplica. Existen cinco (5) acciones posibles:

    a) "*Pass*": Se acepta el paquete sin compararlo con las siguientes reglas.

b) "*Block*": El paquete se destruye directamente sin que el emisor tenga constancia de ello y sin compararlo con ninguna otra política.

c) "*Reinitialize*": El paquete se destruye enviando una señal "TCP RST" o un "*ICMP unreachable*" al receptor, dependiendo de si el paquete es TCP o UDP respectivamente.

d) "*None*": El paquete se compara con las siguientes reglas.

130. Si ninguna regla definida en la política de filtrado aplica al paquete, entonces este se destruye sin notificar al emisor, ya que, el firewall aplica por defecto el modelo de seguridad positiva, según el cual "todo aquello que no está explícitamente permitido, debe prohibirse".

131. Es importante tener en cuenta, que para un conjunto de paquetes IP vinculados al mismo intercambio en capa de transporte (TCP, UDP o ICMP), el dispositivo de *Stormshield* solo comparará el paquete inicial. De forma que cuando se recibe un paquete IP, antes de compararlo con las reglas predefinidas, se comprueba si pertenece a una de las conexiones ya preestablecidas con anterioridad y en caso afirmativo, se dejará pasar sin volver a aplicar el filtrado.

132. Adicionalmente, cuando se configuran funciones de seguridad, el cortafuegos genera políticas de filtrado asociadas a estas, como puede suceder en el caso de las funciones de administración remota del cortafuegos y la configuración de VPNs.

133. La información relacionada con el establecimiento de políticas de filtrado encuentra en la sección "*Filtering and NAT*" del documento **[USER-CONFIG-MANUAL]**. Se puede consultar información adicional en los documentos **[FILTERING-RULE]** y **[NAT-RULE].**

5.14.2 VPN

134. Como se ha venido comentando a lo largo del documento, el cortafuegos permite el establecimiento de comunicaciones basadas en VPN para el intercambio de información a través de redes no controladas, bien sea entre dos cortafuegos o entre el cortafuegos y una estación de trabajo situado en una red que no sea de confianza y que cuente con un cliente de VPN instalado.

135. Mediante el servicio de IPSec, el cortafuegos es capaz de proporcionar control de acceso, integridad y autenticación de la información, protección contra ataques de replicación, y confidencialidad mediante el cifrado de la información.

136. La configuración de IPSec consta de cuatro (4) módulos de configuración:

a) La política de filtrado: Permite crear los túneles IPSec entre dos cortafuegos (*site to site*) o entre un cortafuegos y una estación de trabajo móvil (*Site to remote user*).

b) Pares: Permite crear nuevos pares ("*peers*") introduciendo su perfil IKE, el método de negociación y sus parámetros asociados.

c) Identificación: Permite listar las autoridades de certificación aprobadas utilizando métodos PKI, así como claves precompartidas (PSK).

d) Perfiles de cifrado: Permite definir los perfiles IKE (fase 1) e IPSec (fase 2), añadir nuevos o definir el tiempo de vida (en segundos). Además, se pueden definir propuestas de negociación para algoritmos de cifrado y autenticación.

5.14.2.1 PERFILES DE CIFRADO

137. La confidencialidad y la integridad de los flujos de información en una VPN se basan sobre todo en el uso de algoritmos criptográficos robustos negociados entre las dos partes. El uso de perfiles de cifrado del menú *"VPN → VPN IPsec →Encryption Profiles"* permiten especificar los algoritmos a utilizar.

138. De entre los distintos perfiles predefinidos, el más interesante es el de "*StrongEncryption*", que permite modificar sus parámetros, permitiendo al usuario seleccionar entre los siguientes algoritmos criptográficos para obtener una configuración segura de entre las siguientes posibles configuraciones:

Parámetro	Valor
Algoritmo de cifrado	*AES 256*
Función *Hash*	*SHA 256, SHA 384 o SHA 512*
Grupo *Diffie-Hellman*	*Grupo 15 (3072 bits), Grupo 15 (3072 bits), Grupo 16 (4096 bits), Grupo 17 (6144 bits), Grupo 18 (8192 bits), Grupo 16 (4096 bits), Grupo 19 (256 bits ECC), Grupo 20 (384 bits ECC), Grupo 21 (521 bits ECC)*
Criptoperíodo	*21600s*

Tabla 1: Perfil de cifrado "*StrongEncryption*" modificado para IKE

Parámetro	Valor
Algoritmo de cifrado	*AES 256*
Función *Hash*	*SHA 256, SHA 384 o SHA 512*
Grupo *Diffie-Hellman*	*Grupo 15 (3072 bits), Grupo 15 (3072 bits),*

Parámetro	Valor
	Grupo 16 (4096 bits), Grupo 17 (6144 bits), Grupo 18 (8192 bits), Grupo 16 (4096 bits), Grupo 19 (256 bits ECC), Grupo 20 (384 bits ECC), Grupo 21 (521 bits ECC)
Criptoperíodo	*3600s*

Tabla 2: Perfil de cifrado "*StrongEncryption*" modificado para IPSec

5.14.2.2 INTERCAMBIO DE CLAVES Y AUTENTICACIÓN

139. La protección ofrecida por un túnel VPN IPSec depende de la implementación de una *suite* de cifrado basada en algoritmos criptográficos robustos y un mecanismo confiable de intercambio de claves. **La negociación dinámica de todos los algoritmos y túneles IPSec se debe hacer usando el protocolo IKEv2.**

140. Para evitar cualquier tipo de usurpación, independientemente del tipo de túnel utilizado, es necesario autenticar al corresponsal remoto al crear el túnel. Para ello, es posible realizar la autenticación mediante clave compartida o mediante certificado.

141. Por defecto, no se recomienda el uso de claves precompartidas, salvo que sea posible asegurar que éstas ofrecen la fortaleza mínima requerida (128 o 256 bits, según el caso) y se hayan protegido adecuadamente. En su lugar, se recomienda utilizar certificados, ya que el uso de mecanismos de criptografía asimétrica, especialmente aquellos basados en PKI, permitirán llevar a cabo una identificación de forma precisa pudiendo controlar los derechos y funcionalidades adicionales.

142. Para llevar a cabo la configuración adecuada de la autenticación mediante certificado, es necesario ir a la pestaña "*Identification*" para añadir las Autoridades de Certificación aceptadas Adicionalmente, en la pestaña "*peer*" es necesario definir el certificado que se usará como identificador local en la negociación de la fase 1 hacia el *peer* que se está configurando.

5.14.2.3 POLITICAS DE ENRUTAMIENTO Y FILTRADO SALIENTES Y CONFIGURACION DE VPN IPSEC

143. La definición correcta de las reglas de enrutamiento y filtrado es crítica para garantizar la confidencialidad e integridad de los flujos. Por tanto, como parte de la implementación de los túneles IPSec, es necesario tener una ruta que permita unirse a las redes remotas accesibles a través de túneles. De lo contrario, el paquete se elimina en el paso de enrutamiento y no alcanza el paso cifrado de IPSec.

144. Para llevar a cabo la configuración de túneles IPSec de forma segura, se recomienda:

    a) Configurar una ruta estática vía la interfaz local de *loopback* ("*blackholing*": por ejemplo 127.42.42.42) para unirse a redes remotas accesibles a través de túneles IPSec.

    b) Asegurarse de que la política IPSec nunca se desactive incluso durante las fases transitorias.

    c) Asegurarse de que las reglas de filtrado sean siempre más específicas que las reglas de NAT con la opción "*NAT before IPSec*".

    d) Asegurarse de que las reglas de NAT con la opción "*NAT before IPSec*" siempre se incluyan en la política IPSec.

    e) Asegurarse de que en ausencia de reglas NAT, las reglas de filtrado sean siempre más específicas que la política IPSec.

5.14.2.4 POLÍTICA DE FILTRADO ENTRANTE EN EL CASO DE UNA CONEXIÓN VPN IPSEC

145. Un atacante de la red puede enviar flujos de información al cortafuegos falsificando una dirección IP legítima. Estos mensajes no encapsulados deben ser identificados y rechazados. Para lograrlo, es necesario establecer una regla de filtrado que permita el flujo en claro solo si proviene de un túnel VPN IPSec. Para llevar a cabo esta configuración, es necesario ir al menú *"Security Policy→ Filter-NAT→ Filtering"* y cuando se edita una regla de filtrado, el valor del túnel *VPN IPSec* debe introducirse en el campo *"Source→ Solapa "Advanced Configuration"→ "Vía: IPSEC VPN Tunnel".*

146. De esta forma, las políticas de seguridad de cada túnel IPSec aseguran que los flujos de información sólo pasan a través del túnel que es legítimo para ellos.

5.14.2.4.1 *ANTI-SPOOFING* EN EL TÚNEL IPSEC.

147. El cortafuegos considera los extremos de los túneles VPN IPSec como interfaces no protegidas. Por tanto, se debería seguir el proceso detallado en la sección "5.4.1.1 CONFIGURACIÓN DE IP ANTI-SPOOFING" y declarar las interfaces VPN como "*internas*" para poder utilizar los mecanismos *anti-spoofing* para que junto con la definición de las reglas de filtrado, se consiga aumentar notablemente la seguridad.

5.14.2.5 TÚNELES VPN MÓVILES

148. En este caso, el equipo móvil tiene dirección IP desconocida por lo que no es posible introducir la dirección IP del equipo móvil en la configuración del túnel.

149. Para configurar un túnel VPN con un equipo móvil, es necesario ir al menú *"VPN→ IPSec VPN"* y la pestaña "*Anonymous – Mobile Users*" para proporcionar una IP al dispositivo móvil, de forma que el cortafuegos por medio del modo "*Config Mode On"* pueda enviar la dirección IP al mismo para evitar posibles conflictos con las direcciones IP de otros usuarios.

5.14.2.6 DETECCIÓN DE PARES MUERTOS

150. Este mecanismo realiza una verificación periódica del estado del túnel IKE a través de intercambios de mensajes cifrados. Si un dispositivo no responde a las solicitudes, entonces lo considera como inalcanzable y cerrará el túnel IKE, así como los túneles VPN IPSec asociados.

151. Se recomienda activar el mecanismo de detección de *peers* no accesibles *(dead peer detection*) seleccionando el modo "*high"* o bien seleccionando modo "*low*", en la pestaña "*peers*" dentro del menú *"VPN→IPSec VPN*", ya que, en ambos casos se configurará el cortafuegos para monitorizar el estado del equipo remoto. El modo "*high*" hará que las solicitudes DPD se hagan de forma más frecuente que en modo "*low*". En caso que el equipo remoto no responda a las solicitudes DPD, se cerrará el túnel.

5.14.2.7 KEEPALIVE

152. Cuando un túnel IPSec no se utiliza, es posible fijar un período de tiempo con el fin de liberar recursos en el cortafuegos. Sin embargo, si el túnel se reactiva, entonces es necesario volver a reiniciar las negociaciones, lo cual supone cierta latencia y pérdida de paquetes. Para evitar esta situación el mecanismo *keepAlive* permite generar tráfico artificial en el túnel para mantenerlo activo. Además, es posible llevar a cabo el filtrado de dicho tráfico sin que deje ningún tipo de rastro.

153. Para activar este mecanismo es necesario ir al menú *"VPN→ IPSec VPN→ Encryption Policy - Tunnels"* y haciendo *clic* sobre el encabezado de cualquier columna de la tabla y clicando en el triángulo invertido de la esquina derecha del encabezado de columna aparece la opción "*Column*" para habilitar la columna "*Keep Alive*", pudiendo posteriormente modificar el intervalo de tiempo. Si el valor del intervalo de tiempo es '0', indica que el "*Keep Alive*" no está en curso.

5.14.3 ANTISPAM

154. El cortafuegos permite llevar a cabo la tarea de *antispam* mediante análisis de reputación, es decir, llevando a cabo la validación del emisor mediante la comparación con listas públicas (*DNS Blacklists – DNSBL*) de emisores de *Spam* o mediante análisis heurístico del contenido del propio email para determinar su impacto.

155. Permite llevar a cabo cuatro posibles acciones sobre los mensajes que se identifican como *spam*:

    a) Etiquetarlo como spam: Los emails no se bloquean, pero se etiquetan como spam.

    b) Bloquear todos los mensajes de *spam*: El email será rechazado independientemente del nivel de confianza.

    c) Bloquear todos los mensajes de *spam* a nivel 2 o superior: Esta opción permite definir tres umbrales: Bajo, Medio y Alto.

    d) Bloquear solo a nivel 3: Esta opción permite bloquear los emails que superen el nivel 3.

156. Los niveles de antispam se definen en función de la puntuación del motor heurístico de análisis antispam:

    a. Nivel 1: Antispam *score* 100-200.

    b. Nivel 2: Antispam *score* 200-300.

    c. Nivel 3: Antispam *score* de 300 en adelante.

157. Si se habilita el uso de DNSBL, es necesario tener en cuenta que la lista de servidores utilizados por el cortafuegos se actualiza periódicamente mediante el servicio de actualización activa "*Active Update*" y que no pueden ser modificados, aunque sí se permite deshabilitar el uso de parte de ellos o añadir nuevos.

158. Por otro lado, el análisis heurístico se basa en el uso de tecnología *antispam VadeRetro*, la cual es capaz de calcular el grado de legitimidad del mensaje.

159. Para consultar la información al respecto de cómo proceder con la configuración de la funcionalidad de antispam, es necesario consultar la sección "*Antispam*" del documento **[USER-CONFIG-MANUAL]**.

5.14.4 PREVENCIÓN DE ATAQUES

160. Gracias a su sistema IPS basado en la tecnología ASQ (*Active Secure Qualification*) el producto realiza escaneo dinámico a nivel de IP, transporte y aplicación que, mediante el establecimiento y optimización de reglas, permite la aplicación rápida y segura de las políticas de control de flujo de información, permitiendo:

161. La detección de ataques no orientados a conexión como:

    a) *IP spoofing* mediante el mapeo de la dirección IP de origen a la interfaz en la que se reciben los paquetes.

    b) Falsificación de paquetes como las realizadas mediante *'xmas tree'.*

    c) Superposición de paquetes para evitar las políticas de control de flujo de información.

    d) Intentos de buffer *overflow* a nivel de aplicación.

162. La detección de ataques orientados a conexión:

    a) Uso incorrecto de números de secuencia TCP.

    b) Ataques de fuerza bruta sobre FTP.

163. La detección de ataques que requieran cruce de información de varias fuentes como:

    a) Inundación de recursos en servidores mediante el envío excesivo de solicitudes para la apertura de conexiones TCP (*SYN flooding*).

    b) Intentos de descubrimiento de la topología de red interna haciendo uso de herramientas como *nmap* o QueSO.

164. La siguiente tabla, muestra la lista completa de ataques que el motor ASQ es capaz de manejar:

Nivel de análisis	Nombre del ataque
IP	*IP loopback address spoofing*
	IP address spoofing
	Broadcast Packet
	Multicast Packet
	Address from experimental class
	Bad IP options
	Unknown IP options
	Unanalyzed IP protocol

Nivel de análisis	Nombre del ataque
	Unknown internal network host
	Oversized fragment
	Overlapped fragment
	Multicast address with TCP
	Land style attack
	Source routing
	Detection of the filter policy
	Possible port scan
	Zero sized fragment received
	Tiny fragment
	Port probe
	IP address spoofing on bridge
	Broadcast address with TCP
	Filter alarm
	"Link local" addresses (RFC 3330)
	Broadcast address used in source address
	Possible attack on resources
	Invalid IP protocol
	Blacklisted address
	Whitelisted address
	Packet for destination on the same interface
	Wrong IP checksum
	Quality of service drop
	IP fragment analyze
	IP address spoofing on IPSec interface
	Connection lost
TCP	*Invalid TCP option*
	Unknown TCP option
	Wrong TCP sequence number
	Wrong TCP checksum
	Xmas tree attack

Nivel de análisis	Nombre del ataque
	Nmap OS probe
	Queso OS probe
	Possible TCP SYN flooding
	Port 0 used as service
	Windows OOB data bug
	Possible small MSS attack
	Misplaced TCP option
	TCP data evasion
	TCP data queue overflow
	Interactive connection detection
	Invalid TCP packet for current connection state
	Invalid TCP protocol
	Datatracking problem
	Unauthorized protocol detected
	Urgent unauthorized data in TCP information flows
	Desynchronization of TCP information flows
	Managed by synproxy
	Desynchronization status of TCP information flows
	Cisco WAN information flow optimizer detected
	Possible TCP request flooding
	RFC 2385 MD5 signature for TCP
	Number of connections allowed per host reached
	Number of connections allowed per host per interval reached
UDP	*Possible UDP flooding*
	UDP port loopback
	Port 0 used as service
	Invalid UDP checksum
	Datatracking problem
	Invalid UDP protocol
	Unauthorized protocol detected
	Possible UDP request flooding

Nivel de análisis	Nombre del ataque
ICMP	*Unknown ICMP type*
	ICMP reply without request
	ICMP redirect
	Possible ICMP flooding
	XProbe OS probe
	Invalid ICMP message
	ICMP 'timestamp' request
	ICMP 'mask' request
	Invalid ICMP checksum
	Possible small MTU attack
	ICMP 'information' request
	Allowed by ICMP analyze
	Modification of ECHO ICMP data
	Protocol not analyzed in an ICMP message
IGMP	*Unknown IGMP type*
	Non-multicast address in IGMP query
	Invalid IGMP packet
	Invalid IGMP checksum
DNS	*DNS label recursion*
	DNS id spoofing
	DNS zone change
	DNS zone update
	DNS cache poisoning
	Bad pointer in packet
	Possible buffer overflow using DNS string
	Bad DNS protocol
	Contradictory DNS query field
	Targeted DNS spoofing
	Possible 'DNS rebinding' attack
	Duplicated DNS response
FTP	*Possible FTP bounce attack*

Nivel de análisis	Nombre del ataque
	FTP PASV insertion attack
	Unknown FTP command
	Buffer overflow on FTP USER/PASSWORD
	Buffer overflow on FTP command
	Brute force attack on FTP password
	Command execution using SITE EXEC
	FTP PASV DoS
	Invalid FTP Protocol
	Invalid PORT command
	User not allowed
	Blacklisted user
HTTP	*Invalid %u encoding char in URL*
	Evasion using %u encoding char in URL
	Invalid escaped char in URL
	Escaped NULL char in URL
	Escaped percent char in URL
	Evasion using UTF-8 encoding
	Invalid HTTP protocol
	Possible buffer overflow on URL
	Possible buffer overflow on HTTP request
	Tunneling using CONNECT method
	Multiple slashes in URL
	Directory self-reference
	Directory traversal
	Bad UTF-8 encoding in URL
	Possible malicious code in HTTP header
	Directory traversal outside root folder
	Bounce by redirect
	304 response with data
	Additional data at end of reply
	HTTP parameter pollution attempt

Nivel de análisis	Nombre del ataque
	Unicode character to change reading direction in HTTP URL
	Too many HTTP headers in request
	Unexpected HTTP/1.1 response for this User-Agent
	Decoding of HTML field failed, invalid code
	Recursion detected in decoding of HTML field
	HTTP redirection to local file
	Too many ranges in HTTP request
	Malformed ranges in HTTP request
	Compressed HTTP content
	The URL contains non-ASCII "8bit in request" characters
	RFC 2817 method TLS UPGRADE detected
	RFC 6455 method WebSocket UPGRADE detected
	Capacity exceeded in an HTML attribute
SIP	*Invalid SIP protocol*
	Overflow in SIP protocol
	Possible malicious code in SIP header
	Missing necessary SIP header
	Spoofed SIP request
	Missing necessary SDP field in the SIP protocol
	Invalid SIP expires field
	Bad UTF-8 encoding in the SIP protocol
	SIP operation limit exceeded
	Missing purpose parameter in the SIP protocol
	Bad Via field in the SIP protocol
	Binary packet in the SIP protocol
	Invalid value in SIP Max-Forward header
	Missing SIP Max-Forwards header
	The SIP request contains an invalid "Contact field" "From field" URI
SMTP	*Invalid SMTP protocol*
	Invalid characters in SMTP header

Nivel de análisis	Nombre del ataque
	Overflow in the SMTP protocol
	Invalid parameters for the SMTP BDAT command
	Empty SMTP command line or response
	Invalid base64 data in an AUTH SMTP command SMTP
	SMTP DATA command with parameters
	SMTP command not supported by the server
	SMTP BDAT command disabled
	Exchange Server SMTP commands disabled
	SMTP EXPN command used
	SMTP VRFY command used
	SMTP TURN, ATRN, ETRN commands disabled
	Forbidden SMTP command found
	SMTP message with too many header bytes
	SMTP subject header contains non-ASCII characters
	Brute force attack on SMTP authentication
	Sending of e-mail through an anonymous SMTP connection

Tabla 3: Ataques detectables por el cortafuegos de Stormshield

165. Para llevar a cabo la correcta detección del ataque *ICMP flooding*, el cortafuegos debe ser configurado como se muestra en los siguientes pasos:

a) Ir a "*Configuration → Security Policy → Filter-NAT*" y configurar la regla de la sección "*Default Policy"* con la siguiente configuración:

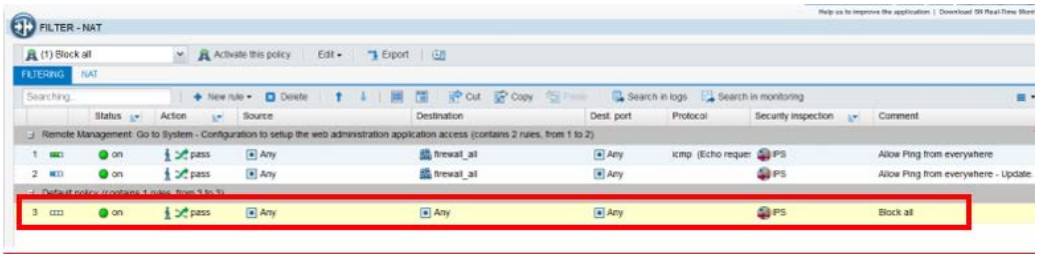

Figura 7: Configuración de la regla de la sección 'Default Policy'.

b) Posteriormente hacer doble *clic* sobre la misma e ir a *"Action → Quality of service"* y en el desplegable correspondiente al *threshold* seleccionar "*Raise Associated Alarm"* y configurar el número de conexiones ICMP por segundo deseadas (Ej: 10) y hacer clic en "Ok":

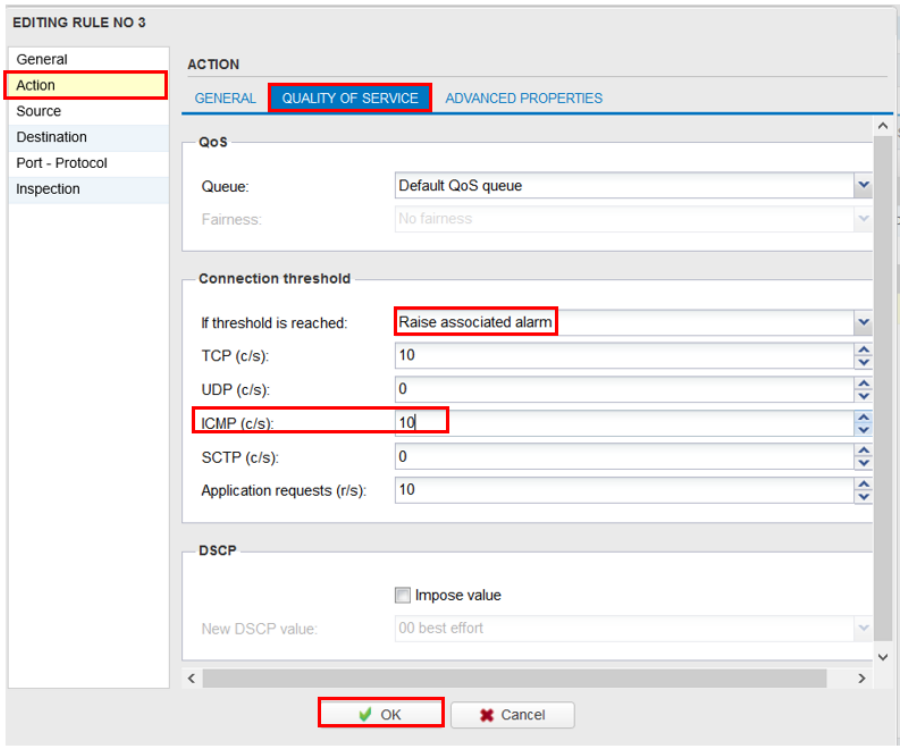

Figura 8: Configuración del número de conexiones ICMP.

c) Posteriormente hacer clic en "*Save and apply*" en la parte inferior de la pantalla para establecer la nueva política de seguridad.

d) Una vez establecida la nueva política de seguridad, solo queda habilitar la protección que la hará efectiva para el IPS_00 y el IPS_01, ya que por defecto está deshabilitada. Para ello, ir a "*Configuration → Applications and protections"* y en el filtro de la zona superior buscar "*Quality of service drop*":

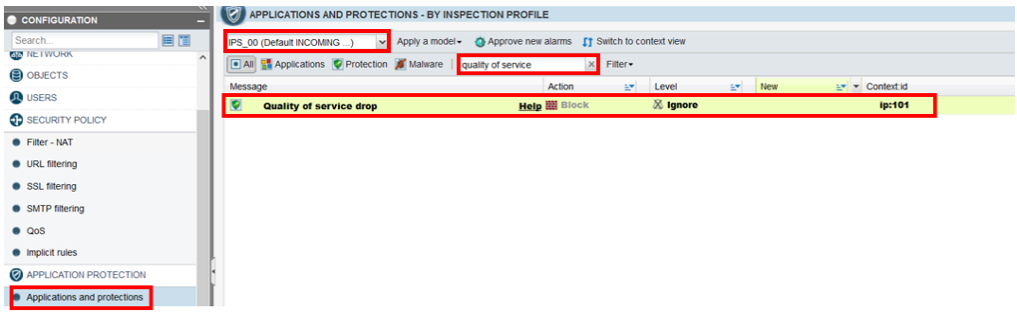

Figura 9: Habilitar protección para IPS_00.

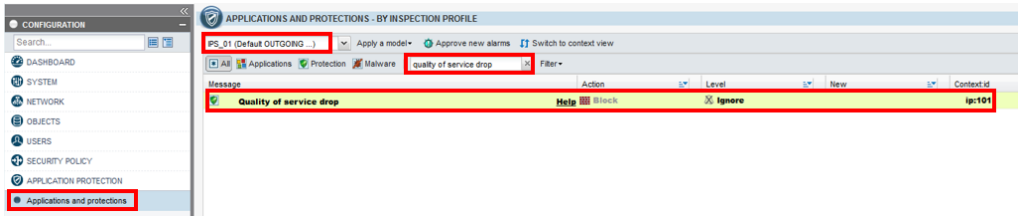

Figura 10: Habilitar protección para IPS_01.

e) Para activarla, pinchar sobre "*Ignore*" y cambiar a "*Major*" y hacer clic en el botón "*Apply*" en la zona inferior de la pantalla:

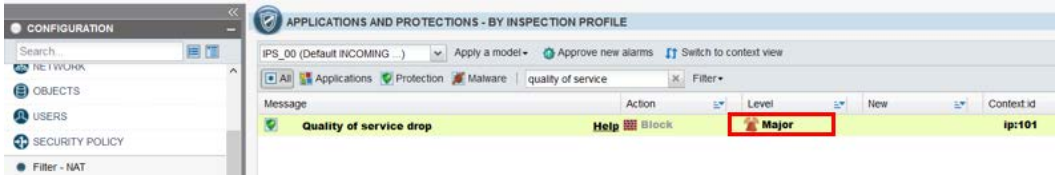

Figura 11: Establecimiento del nivel de alarma a Major para IPS_00.

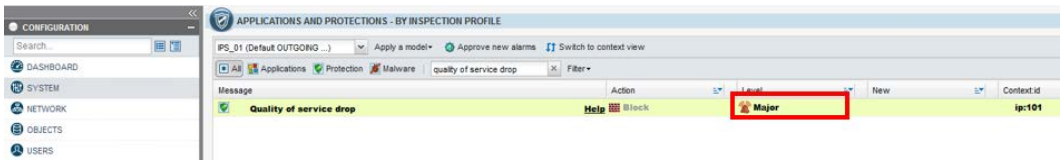

Figura 12:Establecimiento del nivel de alarma a Major para IPS_01.

f) Finalmente, también es necesario limitar la media del tráfico de entrada. Para ello, ir a "*Configuration → Network → Interfaces*" y seleccionar "*out*" que se corresponde con el tráfico que viene de fuera. Ir a la pestaña "*Advanced Configuration*" y en el desplegable "*media*" seleccionar "*10Mbps half duplex*" y pulsar en el botón "*Apply*" en la parte inferior de la pantalla:

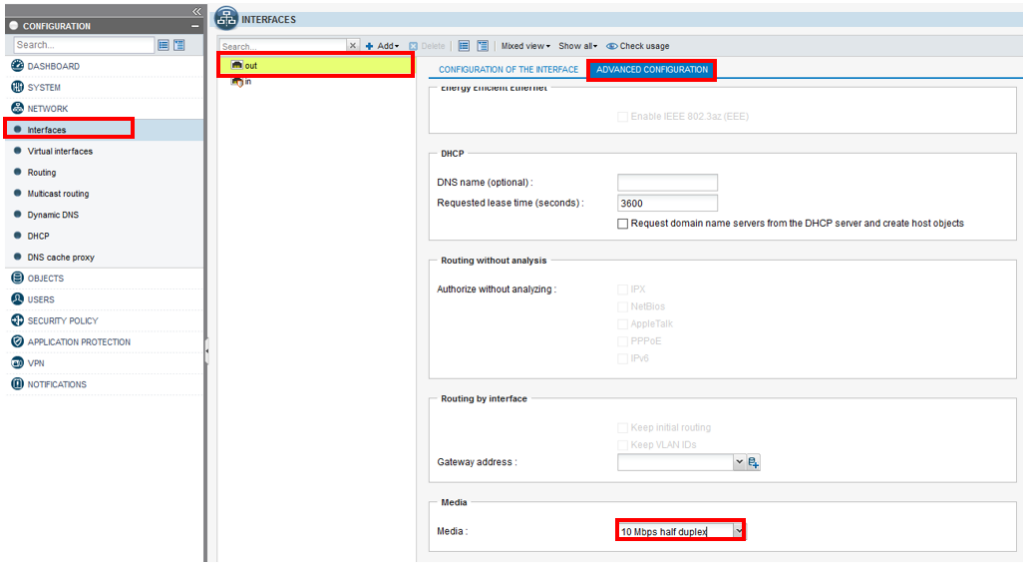

Figura 13: Limitación del tráfico de entrada.

166. Finalmente, para habilitar el IPS y poder llevar a cabo la detección de todos los ataques enumerados anteriormente, es necesario ir al menú *"Filter and NAT→ Security inspection"* y habilitar la opción IPS.

6 FASE DE OPERACIÓN

167. Una vez el cortafuegos está configurado de forma segura y se encuentra en modo de funcionamiento normal, el usuario *super administrador* es el encargado de llevar a cabo las siguientes tareas de mantenimiento:

a) Comprobaciones periódicas del *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.

b) Comprobaciones periódicas de la correcta operación de los algoritmos y funciones criptográficas, a través de la ejecución de los correspondientes auto-chequeos (*self-tests*).

c) Actualizaciones periódicas del software de los equipos, para garantizar que están al día, tanto en las capacidades de reconocimiento de aplicaciones, como en la prevención de amenazas.

d) Realización de backups automáticos de forma periódica y, a poder ser, de forma centralizada.

e) Mantenimiento de los registros de auditoria. Estos registros estarán protegidos de borrados y modificaciones no autorizadas, y solamente el *super administrador* podrá acceder a ellos. La información de auditoria se guardará en las condiciones y por el periodo establecido en la normativa de seguridad.

f) Auditar, al menos, los eventos especificados en la normativa de referencia y aquellos otros extraídos del análisis de riesgos.

7 CHECKLIST

168. La siguiente *checklist* contiene todas las recomendaciones sobre la configuración relativas al cortafuegos de *Stormshield*:

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto	☐	☐	
Instalación en un entorno seguro	☐	☐	
Registro de los equipos	☐	☐	
Registro de las licencias	☐	☐	
Actualización de *firmware*	☐	☐	
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
Modo de Operación seguro activado (FIPS-CC)	☐	☐	
Configuración de la metodología de autenticación	☐	☐	
Configuración segura de red	☐	☐	
Configuración segura de servicios	☐	☐	
Configuración segura de protocolos	☐	☐	
Configuración del sistema de gestión de certificados	☐	☐	
Configuración segura de la función de sincronización horaria	☐	☐	
Configuración segura del protocolo de administración de red *SNMP*	☐	☐	
Configuración del sistema para su funcionamiento en alta disponibilidad (si se requiere)	☐	☐	
Configuración segura del sistema de auditoría (local o externo)	☐	☐	
Configuración segura del sistema de backup	☐	☐	
Establecimiento de las políticas de cortafuegos	☐	☐	

ACCIONES	SÍ	NO	OBSERVACIONES
Configuración segura de VPN IPSec	☐	☐	
Configuración segura del servicio *AntiSpam*	☐	☐	
Configuración segura del servicio IPS	☐	☐	

Tabla 4: *Checklist* de configuración

8 REFERENCIAS

[DAT-NT-001]	Recommandations de sécurité relatives aux mots de passe, V 1.1
[CLI-SERVERD-COMMAND]	CLI Serverd Command reference Guide, v3.10.2
[CLI-CONSOLE/SSH-COMMAND]	CLI Console/SSH Commands Reference Guide, V 3.0
[USER-CONFIG-MANUAL]	User Configuration Manual, V 3.0
[AUDIT-LOG-TEC-NOTE]	Description of Audit logs, V 3
[SNENTNO_AUTOBACKUP]	Automatic Backups V 1.0
[FILTERING-RULE]	Setting up a Filtering Rule, V June 19,2019
[NAT-RULE]	Setting up a NAT Rule, V June 19,2019
[INSTALLATION-GUIDE]	Product presentation and installation 2019, V 1.0
[SAFETY-RULES-SNRANGE]	Safety Rules and Installation Precautions – SN Range, V 2.0
[RGS]	Annexe A1 Règles relatives à la mise en oeuvre des fonctions de sécurité basées sur l'emploi de certificats électroniques.V 1.0
[SVC-ADMIN-GUIDE]	Stormshield Visibility Center Administration Guide, V1.5

9 ABREVIATURAS

ASQ	*Active Secure Qualification*
CLI	*Command Line Interface*
CRL	*Certificate Revocation List*
DNS	*Domain Name Servers*
DNSBL	*DNS BlackList*
ENS	Esquema Nacional de Seguridad.
ESP	*Encapsulating Security Payload*
ICMP	*Internet Control Message Protocol*
IP	*Internet Protocol*
IPS	*Intrussion Prevention System*
IPSec	*Internet Protocol Security*
IT	*Information Technology*
NAT	*Network Address Translation*
PKI	*Public Key Infrastructure*
PSK	*Pre-Shared Key*
SDHC	*Secure Digital High Capacity*
SDXC	*Secure Digital Extended Capacity*
SNS	*Stormshield Network Security*
SSH	*Secure Shell*
TCP	*Transport Control Protocol*
TLS	*Transport Layer Security*
UDP	*User Datagram Protocol*
URL	*Uniform Resource Locator*
VPN	*Virtual Private Network*