Guía de Seguridad de las TIC
CCN-STIC 1421

Procedimiento de empleo seguro
WatchGuard Fireware

Abril de 2024

MINISTERIO DE DEFENSA

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Pº de la Castellana 109, 28046 Madrid
Centro Criptológico Nacional.

NIPO: 083-24-146-X.
Fecha de Edición: abril de 2024

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.04.12 09:47:09 +02'00'

ÍNDICE

1. INTRODUCCIÓN 5
2. OBJETO Y ALCANCE 6
3. ORGANIZACIÓN DEL DOCUMENTO 7
4. FASE DE DESPLIEGUE E INSTALACIÓN 8
4.1 ENTREGA SEGURA DEL PRODUCTO 8
4.2 INSTALACIÓN SEGURA 9
4.2.1 CONFIGURACIÓN POR DEFECTO 9
4.2.2 ASISTENTE DE CONFIGURACIÓN 10
4.2.3 ACTUALIZACIÓN DEL *FIRMWARE* 13
4.3 REGISTRO Y LICENCIAS 13
5. FASE DE CONFIGURACIÓN 15
5.1 HABILITACIÓN DEL MODO CSFC 15
5.2 AUTENTICACIÓN 16
5.2.1 ROLES DE USUARIO 16
5.2.2 CREACIÓN DE UN NUEVO USUARIO 17
5.2.3 POLÍTICA DE CONTRASEÑAS 17
5.2.4 CONFIGURACIÓN DEL BLOQUEO DE CUENTAS DE USUARIO 18
5.2.5 DESBLOQUEO DE CUENTAS DE USUARIO 19
5.2.6 TIEMPO DE FINALIZACIÓN DE SESIÓN 19
5.3 ADMINISTRACIÓN DEL PRODUCTO 20
5.3.1 ADMINISTRACIÓN LOCAL Y REMOTA 20
5.3.2 MENSAJE DE AVISO Y CONSENTIMIENTO 21
5.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 21
5.5 GESTIÓN DE CERTIFICADOS 22
5.6 SINCRONIZACIÓN HORARIA 23
5.6.1 MODIFICACIÓN DE LA ZONA HORARIA 23
5.6.2 CONFIGURACIÓN DE LOS SERVIDORES NTP 24
5.6.3 ACTUALIZACIÓN MANUAL DE LA HORA 24
5.7 AUDITORÍA 25
5.7.1 REVISIÓN DE LOS LOGS DE AUDITORÍA 25
5.7.2 CONFIGURACIÓN DE LOS LOGS DE AUDITORÍA 26
5.7.3 ALMACENAMIENTO REMOTO DE LOGS 29
5.8 SERVIDORES DE AUTENTICACIÓN 29
5.8.1 CONFIGURACIÓN DE DIRECTORIO ACTIVO 29
5.9 ACTUALIZACIONES 30
5.10 AUTO-CHEQUEOS 31
5.11 *BACKUP* 32
5.12 POLÍTICAS DE CORTAFUEGOS 32
5.12.1 POLÍTICAS Y SERVICIOS DE CORTAFUEGOS POR DEFECTO 33
5.12.2 PROTECCIÓN ANTE AMENAZAS POR DEFECTO 33
5.12.3 MANEJO DE PAQUETES POR DEFECTO 34
5.12.4 SITIOS BLOQUEADOS 35
5.12.5 CONFIGURACIÓN DE LAS POLÍTICAS DE CORTAFUEGOS 37

5.12.6 ORDEN DE PREFERENCIA DE LAS POLÍTICAS 43
5.12.7 POLÍTICAS OCULTAS 45
5.12.8 CONFIGURACIÓN DE POLÍTICAS OBLIGATORIA 45
5.13 VPN IPSEC 49
5.13.1 CONFIGURACIÓN DE UN *GATEWAY BOVPN* 50
5.13.2 CONFIGURACIÓN DE UN TÚNEL BOVPN 56
5.13.3 AUTENTICACIÓN MEDIANTE CERTIFICADOS PARA BOVPN 59
5.13.4 AÑADIR POLÍTICAS DE CORTAFUEGOS AL TRÁFICO VPN 61
6. FASE DE OPERACIÓN 62
***7. CHECKLIST* 63**
8. REFERENCIAS 64
9. ABREVIATURAS 65

TABLAS

Tabla 1 Plataformas Compatibles 6
Tabla 2 Comportamiento de descarte de paquetes según límite configurado 35

ILUSTRACIONES

Ilustración 1 – Interfaces de conexión para la configuración inicial. 11
Ilustración 2 - Activación de Producto 14
Ilustración 3 - Modificación de la Zona Horaria. 23
Ilustración 4 - Configuración de los servidores NTP 24
Ilustración 5 - Eventos de Auditoría 25
Ilustración 6 - Eventos para las políticas de *proxy* 27
Ilustración 7 - Configuración de la funcionalidad de auditoría 28
Ilustración 8 - Configuración del Nivel de Diagnóstico. 28
Ilustración 9 - *Default Packet Handling* 34
Ilustración 10 - *Blocked Sites* 36
Ilustración 11 - *Firewall Policies* 38
Ilustración 12 - *Add Policy* 38
Ilustración 13 - *Policy Template* 39
Ilustración 14 - *Policy Configuration* 40
Ilustración 15 – *Disposition* 41
Ilustración 16 - *Member Type* 42
Ilustración 17 - Habilitación de los Eventos de las Políticas. 43
Ilustración 18 - Orden automático de preferencia 44
Ilustración 19 - Save Policy Order. 44
Ilustración 20 - Añadir política personalizada 47
Ilustración 21 - Configuración de la política 47
Ilustración 22 - Añadir Número de Protocolo 48
Ilustración 23 - Configuración del Gateway. 50
Ilustración 24 – Añadir un *Gateway Endpoint* 51
Ilustración 25 - Configuración del Punto de Acceso 52

Ilustración 26 - Configuración del Punto de Acceso Remoto 53
Ilustración 27 - Configuración Fase 1 IPSec 54
Ilustración 28 - Configuración de la transformación 55
Ilustración 29 - Configuración de rutas del túnel 57
Ilustración 30 - Configuración de nueva propuesta en Fase 2 59
Ilustración 31 - Aplicación de política de cortafuegos a un túnel 61

1. INTRODUCCIÓN

1. Las plataformas ***WatchGuard Firebox Next Generation Firewall (NGFW)*** ejecutando el *firmware* ***WatchGuard Fireware OS v12.10*** proveen un amplio rango de servicios de red, entre los que destacan sus funcionalidades de *firewall* y VPN. Estos dispositivos incluyen el *hardware*, *firmware* y *software* necesario para desempeñar toda su funcionalidad de manera autónoma.
2. Proveen capacidades de administración local mediante consola y administración remota a través de sus servicios web (mediante HTTPS) sin la necesidad de emplear ningún *software* o dispositivo de administración adicional.
3. El producto proporciona un control de la conectividad entre dos o más entornos de red, siendo capaz de enrutar el tráfico entre las distintas redes y de aplicar distintas reglas de control sobre los flujos de tráfico que se generan entre las mismas con el objetivo de disminuir el riesgo de ataque. La plataforma soporta el filtrado de paquetes de múltiples protocolos, incluyendo ICMPv4, ICMPv6, IPv4, IPv6, TCP y UDP entre otros, siendo capaz de aplicar reglas sobre algunos protocolos de la capa de aplicación como HTTP o FTP.
4. Se permite el establecimiento de túneles VPN empleando el protocolo IPSec en su modo ESP, implementando reglas SPD (permitir, denegar, bypass) que pueden ser configuradas para el distinto tratamiento del tráfico en conjunto con las reglas de *firewall*.
5. Adicionalmente, los dispositivos son capaces de almacenar el estado de los paquetes que cumplen o incumplen cada regla establecida en los registros de auditoría del sistema.

2. OBJETO Y ALCANCE

6. En la presente guía se recoge el procedimiento de empleo seguro del *firmware* ***WatchGuard Fireware OS v12.10*** ejecutándose sobre las plataformas ***WatchGuard Firebox Next Generation Firewall (NGFW)*** para las funcionalidades de cortafuegos y VPN IPSec.

7. En la siguiente tabla se muestran las plataformas que componen el producto y están cubiertas por este procedimiento de empleo seguro:

Versión del *firmware*	Modelos *hardware*	Características *hardware*
Fireware OS 12.10	**T35**	*NXP T1024 (PPC) – e500*
	T40 **T20**	*NXP Layerscape LS1023A, LS1043A – ARM Coretex-A53*
	T80	*NXP Layerscape LS1046A – ARM Coretex-A72*
	T55 **T70**	*Intel Celeron N3060, N3160 (x86) – Braswell*
	M270	*Intel Atom C3558 (x86) – Denverton*
	M370	*Intel Celeron G3900 (x86) – Skylake*
	M470	*Intel Pentium G4400 (x86) – Skylake*
	M570	*Intel Core i3-6100 (x86) – Skylake*
	M670	*Intel Skylake E3-1225v5 (x86) – Haswell*
	M4600	*Intel Xeon E3-1275V3 (x86) – Haswel*
	M5600	*Intel Xeon E5-2680V2 (x86) – Ivy Bridge*

Tabla 1 Plataformas Compatibles

3. ORGANIZACIÓN DEL DOCUMENTO

8. El presente documento se divide en los siguientes apartados que, fundamentalmente, servirá de guía en la configuración segura de la solución *WatchGuard Fireware OS 12.10*:

   a) **Apartado 4**. En este apartado se recogen los requisitos o recomendaciones asociadas a la fase de **despliegue e instalación física** del producto.

   b) **Apartado 5**. En este apartado se recogen requisitos o recomendaciones asociadas a la fase de **configuración segura** del producto.

   c) **Apartado 6**. En este apartado se recogen requisitos o recomendaciones asociadas a la fase de **operación**.

   d) **Apartado 7**. En este apartado se recoge una *checklist* con las tareas a realizar y el estado de cada una de ellas.

   e) **Apartado 8**. Referencias utilizadas en el presente documento.

   f) **Apartado 9**. En este apartado se hace referencia a las diferentes nomenclaturas utilizadas.

4. FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

9. Para asegurar una correcta recepción del producto será necesario revisar que no ha sido manipulado de manera alguna durante su transporte. Para ello, se llevarán a cabo los siguientes pasos:

    a) Antes de abrir el paquete, comprobar que el logo y los motivos de *WatchGuard* están impresos en él. En caso contrario, contactar con el proveedor del producto.

    b) Comprobar que el paquete no ha sido abierto y vuelto a sellar. Esto se puede confirmar examinando los sellos de empaquetado. *WatchGuard* emplea cinta *tamper-evident* para sellar los paquetes enviados. En caso de que parezca que el paquete ha sido sellado más de una vez, contacte con el proveedor del producto.

    c) Comprobar que la caja tiene una etiqueta blanca con un código de barras, el número de producto, número de serie y modelo y otra información relacionada con el contenido de la caja. El objetivo de esta etiqueta es evitar la alteración del interior del paquete. Si se observa que la etiqueta está rota o no está, contacte con el proveedor del producto.

    d) Comprobar que la caja fue enviada por el proveedor esperado. Esto puede comprobarse confirmando con el proveedor que la caja ha sido enviada con la compañía de transportes que ha entregado la caja y comprobando que el número de serie de los elementos enviados coincide con el número de serie de los elementos recibidos. El número de seguimiento del pedido se envía automáticamente al cliente cuando el paquete ha sido enviado.

    e) Una vez el producto se ha desempaquetado, se deberá inspeccionar la unidad y comprobar que el número de serie que aparece en el propio producto coincide con el número de serie de la documentación de envío. Esta comprobación se podrá realizar de la siguiente forma:

        - Físicamente mediante la etiqueta con el número de serie en la parte inferior del dispositivo.
        - Mediante la interfaz CLI usando el comando *sysinfo*.
        - A través de la interfaz web navegando a *Dashboard* > *Front Panel*.

4.2 INSTALACIÓN SEGURA

10. Será imprescindible llevar a cabo la configuración inicial del producto en un entorno seguro y aislado antes de desplegarlo en una red externa.
11. Una vez instalado, el dispositivo deberá encontrarse en un Centro de Proceso de Datos (CPD) seguro que garantice la seguridad física del mismo mediante la limitación del acceso a un conjunto limitado de personas. Para ello, la sala deberá estar dotada de un sistema de control de acceso que asegure que únicamente el personal autorizado puede acceder al dispositivo.
12. El producto se entrega con una imagen del *firmware* precargada. Sin embargo, la imagen puede no encontrarse en la versión 12.10, objeto de esta guía.
13. Con el objetivo de comprobar si la versión instalada es la correcta o de instalar la versión correcta en caso contrario, se deben seguir los pasos indicados en las siguientes subsecciones (ver apartado 4.2.3 ACTUALIZACIÓN DEL *FIRMWARE*). De esta forma se verificará que el entorno es estable y, en caso de necesitarse, se instalará la versión evaluada del producto.

4.2.1 CONFIGURACIÓN POR DEFECTO

14. El producto se entrega con la siguiente configuración inicial, que es necesario conocer cuando se inicia el proceso de instalación y configuración:

    - **Interfaces:**
        - La interfaz 0 se encuentra habilitada como interfaz externa (WAN), actuando como cliente DHCP.
        - La interfaz 1 se encuentra habilitada como interfaz interna, con la dirección IP 10.0.1.1 y con un servidor DHCP habilitado.
        - El resto de interfaces se encuentran habilitadas como interfaces opcionales que podrán ser configuradas una vez se haya finalizado el proceso de instalación y configuración del dispositivo.
    - **Web UI:**
        - El puerto por defecto para establecer conexiones a través de la interfaz web es el puerto 8080.
        - Para conectarse a la interfaz de administración web, el usuario debe conectar un dispositivo actuando como cliente DHCP al puerto 1 del producto y acceder a la siguiente dirección: *https://10.0.1.1:8080*.
        - En la mayoría de los modelos *hardware*, el puerto de administración a través del cual se podrá acceder a la interfaz web será en puerto 32. Adicionalmente, para este modelo, la dirección en la que se encontrará la interfaz será *https://10.0.32.1:8080*.

- **Consola:**
  - Los administradores pueden conectarse al producto a través del puerto serie de consola que se encuentra en la parte posterior del dispositivo empleando las credenciales de un usuario administrador. El usuario debe conectarse al puerto serie empleando un *Baud Rate* de 115200 bit/s. La guía de comandos de *Fireware* [REF1] provee una lista completa de los comandos que se pueden ejecutar a través de esta interfaz.
- **SSH:**
  - La interfaz de administración mediante SSH se encuentra habilitada a través del puerto 4118. Sin embargo, las conexiones a través del puerto SSH no están recomendadas para administrar el dispositivo, por lo que **no se deberá acceder a través de esta interfaz para realizar ninguna operación de administración durante la fase de operación del producto**.
- **Credenciales por defecto:** Los usuarios de administración con los que cuenta el producto son los siguientes.
  - Administrador del dispositivo con acceso de lectura-escritura:

    Nombre de usuario: ***admin***

    Contraseña: ***readwrite***
  - Auditor del sistema con acceso de lectura:

    Nombre de usuario: ***status***

    Contraseña: ***readonly***

15. Una vez se haya iniciado el proceso de configuración inicial, será posible modificar la configuración del dispositivo siguiendo los distintos pasos indicados en el apartado 5 FASE DE CONFIGURACIÓN. Adicionalmente, se deberán cambiar tan pronto como sea posible las credenciales por defecto del dispositivo, para ello consultar el apartado 5.2.3.1 CAMBIO DE CONTRASEÑAS.
16. Por defecto, no se permiten las conexiones a la interfaz de administración web desde la red externa (interfaz 0).

4.2.2 ASISTENTE DE CONFIGURACIÓN

17. El asistente de configuración **permite establecer una configuración de red y de contraseñas en el dispositivo.** También permite configurar de forma automática las políticas y servicios con las opciones recomendadas.
18. Para iniciar el asistente de configuración se debe conectar el dispositivo a un ordenador y a una red con acceso a internet, como se muestra en la siguiente imagen:

Ilustración 1 – Interfaces de conexión para la configuración inicial.

19. Para realizar esta conexión y encender el dispositivo se pueden seguir los siguientes pasos:
    a) Conectar la interfaz 0 a una red con acceso a internet y un servidor DHCP.
    b) Encender el dispositivo conectándolo a la red eléctrica y poniendo el botón de *power* en la posición "I".
    c) Conectar la interfaz 1 al ordenador. El ordenador debe estar configurado para actuar como cliente DHCP, en cuyo caso se le asignará una dirección IP.
    d) En caso de que el ordenador no esté configurado para usar DHCP, se puede cambiar su dirección IP a una de las direcciones de la subred en la que se encuentra la interfaz 1 (10.0.1.0/24).
20. Para **iniciar el asistente de configuración** y realizar la configuración inicial, se deben seguir los siguientes pasos:
    a) Desde el ordenador conectado al producto se debe abrir un navegador y acceder a la dirección *https://10.0.1.1:8080*. El navegador informará al usuario de que el certificado no es confiable debido a que se trata de un certificado que se firma a sí mismo. El usuario debe ignorar dicha advertencia y acceder al servicio web del producto por primera vez. Posteriormente se indicará como modificar los certificados del dispositivo (apartado 5.5 GESTIÓN DE CERTIFICADOS).
    b) Acceder como usuario administrador a la interfaz web, introduciendo las credenciales del administrador por defecto (usuario: ***admin***, contraseña: ***readwrite***) en la página de acceso.
    c) Seleccionar *New Configuration* y aceptar el *End User License Agreement*.
    d) Seguir los pasos del asistente de configuración para establecer la configuración inicial:
        - Configurar la interfaz externa. Se debe configurar el método que usará el dispositivo para establecer una dirección IP en la interfaz externa. Las opciones son:
            - DHCP
            - PPPoE
            - Static

- Configurar servidores DNS y WINS (Opcional). Se debe configurar el dominio DNS y la dirección del servidor WINS si se quiere que el dispositivo las use.
- Configurar la interfaz de confianza. Se debe introducir la dirección IP de la interfaz interna y elegir si se desea habilitar el servidor de DHCP o no, especificando el rango de direcciones IP del mismo.
- Activar el punto de acceso Wireless (solo en los *appliances* que soporten dicha funcionalidad). Se debe desmarcar la casilla para que no se habilite el punto de acceso.
- Configurar contraseñas para el producto. Se deben introducir las nuevas contraseñas de las cuentas ***admin*** y ***status***. Las contraseñas deben cumplir con lo indicado en el apartado 5.2.3 POLÍTICA DE CONTRASEÑAS.
- Activar la administración remota (Opcional). Se debe dejar deshabilitada esta opción.
- Configurar un contacto y seleccionar los ajustes del *Feedback*. Se debe introducir el nombre del dispositivo, localización (opcional) y persona de contacto (opcional) con el objetivo de almacenar información de administración en el dispositivo. Adicionalmente, se debe desmarcar la casilla de envío de información de diagnóstico a *WatchGuard*.
- Configurar la zona horaria. Se debe seleccionar la zona horaria en la que se encontrará situado el dispositivo.
- Añadir la clave de activación. Si el dispositivo no logra conectarse a *WatchGuard* para descargar la clave de activación automáticamente, el usuario puede introducir la misma de forma manual seleccionando la opción "*Add the feature key*" (en el apartado 4.3 REGISTRO Y LICENCIAS se indica cómo obtener dicha clave).

  El usuario puede adquirir una clave de activación a través de la página "*Product Details*" en la cuenta de usuario de WatchGuard, a la que se puede acceder desde la página www.watchguard.com.

  Este paso se puede saltar si no se dispone de una clave de activación en el momento, ya que la misma podrá ser introducida posteriormente. Sin una clave de activación el producto, solo permitirá una conexión desde la red interna a la externa y no proporcionará a acceso a los servicios de suscripción.
- Servicios suscritos. El producto mostrará la lista de los servicios licenciados asociados a la licencia introducida y los activará de forma automática.

  Para el servicio *WebBlocker*, el producto pedirá que se seleccionen las categorías que se quieren bloquear. Dicha configuración podrá ser configurada más tarde.

- Resumen. El producto mostrará un resumen de la configuración aplicada.

21. Una vez se aplique la configuración, el dispositivo deberá quedar configurado de la siguiente manera:
    - Se permitirán las conexiones FTP, ICMP Ping, DNS, TCP y UDP desde la red interna a la red externa.
    - Se bloqueará cualquier tráfico desde la red externa que no haya sido previamente requerido desde la red interna.
    - Se inspeccionará el tráfico FTP, HTTP y HTTPS hacia el exterior.
    - Se emplearán los servicios asociados a la licencia para proteger la red interna.

4.2.3 ACTUALIZACIÓN DEL *FIRMWARE*

22. Una vez establecida la configuración inicial se debe comprobar si la versión del *firmware* incluido es la correcta.
23. Se accederá nuevamente a través de la página web de administración y se comprobará la versión del dispositivo navegando a *Dashboard* > *Front Panel*. En la parte de la derecha de la página se podrá observar **la versión del producto**, que **deberá ser 12.10**.
24. Si la versión del dispositivo coincide con la indicada se podrá pasar a la fase de configuración. En caso contrario deberán realizarse los pasos para actualizar el *firmware* indicados en la sección 5.9 ACTUALIZACIONES.

4.3 REGISTRO Y LICENCIAS

25. Tras la adquisición de un dispositivo, se deberá activar el mismo en la página de activación de WatchGuard. De esta manera, también se activará la garantía del producto y se obtendrá la posibilidad de recibir soporte técnico de parte de WatchGuard.
26. Para ello, se deberá acceder a www.watchguard.com/activate. En dicha página, el usuario deberá acceder con sus credenciales de la cuenta de WatchGuard o registrarse creando una cuenta nueva.
27. Una vez se haya accedido a la cuenta de WatchGuard, se deberá introducir en la pantalla de activación de productos el código serie del producto adquirido:

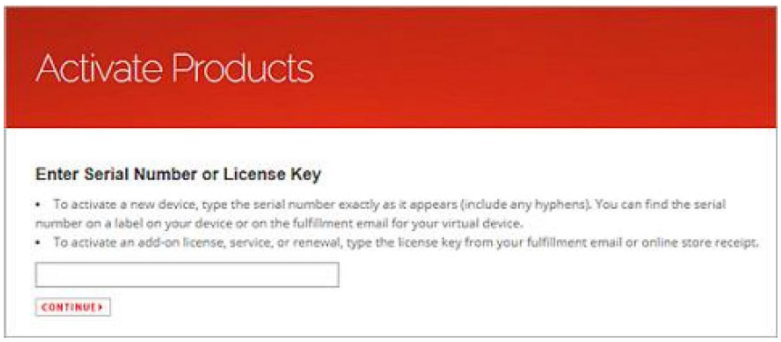

Ilustración 2 - Activación de Producto

28. Se hará clic en continuar y se indicará un nombre para identificar el producto dentro de la página web.
29. Una vez activado, el producto aparecerá en la lista *Manage Product* de la cuenta de WatchGuard del usuario.
30. El proceso de activación generará una clave (*feature key*) que permitirá configurar las características y servicios adquiridos durante la compra del producto.
31. Si el dispositivo se encontrase conectado a internet durante el proceso de instalación del mismo, el propio dispositivo se conectará automáticamente al servicio de activación de WatchGuard y se activará la licencia.
32. En caso de que no se disponga de una conexión a internet, se podrá guardar una copia de la clave de activación (*feature key*) desde la cuenta de usuario de WatchGuard, seleccionando el producto de la lista *Manage Product* y accediendo a la página *Product Details* del mismo. Esta clave se deberá usar durante el proceso de instalación del producto para activarlo.

5. FASE DE CONFIGURACIÓN

5.1 HABILITACIÓN DEL MODO CSFC

33. **Con el objetivo de establecer una configuración segura en el dispositivo, se debe habilitar el modo Common Criteria (modo CSfC)**. Para activar este modo se debe acceder al dispositivo a través de la interfaz de CLI. Para ello, es necesario conectar un ordenador al puerto de consola del producto mediante un cable serie a USB y utilizar una aplicación que sirva como cliente, como por ejemplo *PuTTY*.

34. En la aplicación se configurará el tipo de terminal a VT100 si existe esa posibilidad y se fijarán los siguientes parámetros de la conexión serie:

    - *Baud Rate: 115200.*
    - *Data Bits: 8.*
    - *Stop Bits: 1.*
    - *Parity: None.*
    - *Flow Control: None.*

35. Se abrirá una conexión desde la aplicación y se introducirán las credenciales del usuario administrador (*admin*) para acceder.

36. Una vez en la consola, se introducirá el siguiente comando: *csfc enable*.

37. El dispositivo se reiniciará y se activará el modo CSfC, que habilitará las verificaciones de integridad durante el arranque (apartado 5.10 AUTO-CHEQUEOS) y establecerá los siguientes requisitos criptográficos necesarios para que el dispositivo opere de forma segura:

    1. Comprobaciones de integridad durante el arranque: El dispositivo se apagará inmediatamente durante el arranque si dichas comprobaciones fallan.
    2. Comprobaciones de la integridad de los ficheros de actualización: Se comprobará la firma de los ficheros de aactualización, no realizandose la misma si la verificación falla.
    3. Se habilitará el uso de TLS1.2, quedando desactivado por defecto TLS1.3 y versiones anteriores de TLS.

38. Además, cuando el modo CSfC está activado, algunas de las funcionalidades son modificadas:

    a) Para realizar la conexión con la consola CLI, se deberá hacer uso de un cable de red conectado al puerto de consola. Es decir, **se deshabilitará el acceso mediante SSH.**

    b) La *Firebox* realiza chequeos de integridad durante el inicio del sistema y antes de cualquier actualización. Esto se encuentra explicado en mayor detalle en el apartado 5.10 Auto-Chequeos.

c) La *Firebox* no puede auto-restaurar una imagen de copia de seguridad cuando se inicia en el modo *recovery*.

5.2 AUTENTICACIÓN

39. El sistema solo permite la autenticación de los usuarios mediante la introducción de un usuario y contraseña válidos, no permitiéndose la autenticación mediante certificados.

40. El producto utiliza por defecto su base de datos interna para autenticar a dichos usuarios, siendo esta la configuración recomendada.

41. De forma adicional, el producto permite el uso de servidores externos de Directorio Activo para la autenticación de los usuarios. El proceso de configuración de los servidores de Directorio Activo se encuentra definido en la sección 5.8 SERVIDORES DE AUTENTICACIÓN.

5.2.1 ROLES DE USUARIO

42. La administración del producto basada en roles permite la creación de diferentes usuarios asignados a esos roles, de forma que se pueden repartir las responsabilidades de configuración y monitorización entre diferentes individuos.

43. El producto dispone de los siguientes roles que pueden ser asignados a usuarios:

    - *Device Administrator*: Las cuentas asignadas a este rol pueden conectarse al dispositivo con permisos de lectura y escritura, de forma que pueden cambiar la configuración del mismo y acceder a sus logs.
    - *Device Monitor*: Las cuentas asociadas a este rol solo pueden acceder al dispositivo en modo lectura. De esta manera, solo pueden observar la configuración aplicada y acceder a los *logs* sin realizar ningún cambio en el dispositivo.
    - *Guest Administrator*: Los usuarios asignados a este rol solo pueden conectarse al dispositivo para administrar la lista de usuarios que podrán conectarse al punto de acceso que proporciona el producto si este está activado. En la configuración aplicada esta funcionalidad se encuentra deshabilitada.

44. El producto incluye por defecto tres cuentas de usuario, las cuales no pueden ser eliminadas:

    - *admin*: Cuenta por defecto para el rol de *Device Administrator*, con permisos de lectura y escritura, cuya contraseña es *readwrite*.
    - *status*: Cuenta por defecto para el rol *Device Monitor*, con permisos solo de lectura, y cuya contraseña es *readonly*.
    - *wg-support*: Cuenta de usuario para el acceso del soporte WatchGuard al dispositivo. Esta cuenta está desactivada por defecto y no tiene ninguna contraseña establecida.

45. Dichas contraseñas por defecto se pueden modificar tras acceder con el usuario en cuestión siguiendo los pasos indicados en el apartado 5.2.3.1 CAMBIO DE CONTRASEÑAS.

5.2.2 CREACIÓN DE UN NUEVO USUARIO

46. A la hora de crear usuarios nuevos, solo se pueden crear con los roles vistos anteriormente: *Device Administrator, Device Monitor* o *Guest Administrator.*

47. La creación de usuarios con el rol *Guest Administrator* sólo se puede llevar a cabo en caso de que se haya habilitado la funcionalidad de punto de acceso. Tal como se ha visto en el apartado 4.2.2 ASISTENTE DE CONFIGURACIÓN, no se recomienda el uso de esta funcionalidad.

48. Para la configuración segura, todas las cuentas de usuario deberán usar como servidor de autenticación *Firebox-DB* (la BBDD de datos de usuarios del propio producto). Es importante saber que cuando se crea un nuevo usuario que hace uso del servidor de autenticación *Firebox-DB*, es necesario especificar una contraseña inicial.

49. Para añadir un nuevo usuario al producto, se deberá acceder a través del servicio web con un usuario con permisos *Device Administrator* y navegar a *System > Users and Roles*. Se hará clic en *Add* y se introducirán los siguientes datos:

    - *User Name:* El nombre de la nueva cuenta de usuario.
    - *Authentication Server:* El servidor contra el que se autenticará el usuario. Se debe elegir *Firebox-DB*.
    - *Role*: Se seleccionará uno de los roles de usuario de la lista.
    - *Passphrase*: La contraseña del usuario.
    - *Confirm Passphrase***:** Se volverá a especificar la contraseña del usuario.

50. Se confirmarán los cambios haciendo clic en *OK* y *Save***.**

5.2.3 POLÍTICA DE CONTRASEÑAS

51. Como se ha mencionado en la configuración inicial, el producto permite la gestión de la política de contraseñas. Las contraseñas deberán seguir las siguientes recomendaciones:

    - Deben tener una longitud igual o superior a 12 caracteres.
    - Deberán estar compuestas por una combinación de letras mayúsculas y minúsculas, números y caracteres especiales (“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”).
    - No deberán usarse nombres propios de familiares o personas conocidas ni fechas relacionadas con los mismos.
    - No deberán usarse como contraseña nombres de usuario, ni variantes del mismo.

- Deberán cambiarse de forma periódica. En el caso de contraseñas administrativas, no se debe mantener la misma contraseña por más de 60 días.
- Las nuevas contraseñas deben diferir en, al menos, 4 caracteres, de la contraseña anterior y se debe evitar utilizar contraseñas previamente utilizadas.
- Deberán ser privadas y no compartirse.

52. El único parámetro configurable por el dispositivo es la longitud de las contraseñas. Por defecto, el producto acepta contraseñas con una longitud mínima de 8 caracteres. Para forzar una longitud mínima diferente se deberá:
    a) Acceder al producto a través del servicio web y navegar a *Authentication > Servers.*
    b) Seleccionar *Firebox-DB* e introducir el número mínimo de caracteres en el campo *Minimum passphrase length* (los valores aceptados van de 8 a 32 caracteres). En la configuración evaluada se deberá establecer un tamaño **mínimo de 12 caracteres**.
    c) Finalmente se hará clic en *Save*.
53. Los cambios serán aplicados la próxima vez que se realice un cambio de contraseña para un usuario existente o se cree un nuevo usuario.
54. El resto de las recomiendaciones de seguridad asociadas a la política de contraseñas, deberán ser aplicadas de forma manual.

5.2.3.1 CAMBIO DE CONTRASEÑAS

55. Una vez modificada la longitud mínima de la contraseña, se deberá cambiar la contraseña de los usuarios ya existentes, si estas no cumplen los requisitos mínimos.
56. Para ello se deberán seguir los siguientes pasos:
    a) Acceder al dispositivo a través de la interfaz web (Web UI).
    b) Ir a *System > Users and Roles*.
    c) Seleccionar el usuario cuya contraseña debe ser modificada y hacer clic en *Edit*.
    d) Se introducirá su nueva contraseña en las casillas *Passphrase* y *Confirm Passphrase.*
    e) Finalmente se hará clic en *OK* y *Save*.

5.2.4 CONFIGURACIÓN DEL BLOQUEO DE CUENTAS DE USUARIO

57. Con el objetivo de evitar ataques de fuerza bruta **se debe activar el bloqueo de cuentas de usuario tras un número determinado de intentos de autenticación**.

58. Esta configuración permitirá el bloqueo temporal de las cuentas de usuario por un periodo de tiempo establecido tras superar el número indicado de intentos de autenticación.

59. Para configurar el bloqueo de usuarios se debe acceder a través de la interfaz web y navegar a *System > Users and Roles*. En ese menú se seleccionará la pestaña *Account Lockout* y se marcará la casilla *Enable Account Lockout*. Adicionalmente, deben rellenarse los siguientes campos:

    a) *Failed login attempts*: Se indicará el número de intentos de autenticación consecutivos antes de que se bloquee la cuenta. Para una configuración segura se establecerá un número de intentos **no superior a 3.**

    b) *Users locked out for*: En esta casilla se indicarán los minutos que la cuenta permanecerá bloqueada. En la configuración segura este número debe ser de, al menos, **5 minutos o mayor**.

    c) *Temporary lockouts*: Esta casilla indicará el número de bloqueos temporales que se producirán antes de que la cuenta se bloquee permanentemente. En la configuración evaluada este valor deberá ser **5 o menor**. Cabe destacar que el bloqueo permanente de la cuenta no aplica a la cuenta de administración por defecto, de forma que no es posible bloquear el acceso al dispositivo permanentemente.

    d) Finalmente se hará clic en *Save*.

60. Se ha de notar que el usuario por defecto *admin* puede bloquearse de manera temporal para las conexiones a la interfaz Web UI, pero no se puede bloquear permanentemente. Cuando se activa el modo CSfC, la cuenta del usuario *admin* nunca se bloquea para las conexiones a la CLI a través del puerto de consola.

5.2.5 DESBLOQUEO DE CUENTAS DE USUARIO

61. En caso de que una cuenta de usuario quede bloqueada permanentemente, esta solo podrá ser desbloqueada por un usuario con permisos de administración.

62. Para desbloquear una cuenta se debe:

    a) Acceder al producto a través de su interfaz web (Web UI).

    b) Ir a *System > Users and Roles*.

    c) Seleccionar la cuenta bloqueada y hacer clic en el botón *Unlock*.

    d) Tras ello, hacer clic en *Yes* y la cuenta quedará desbloqueada.

5.2.6 TIEMPO DE FINALIZACIÓN DE SESIÓN

63. Los usuarios con el rol de administración pueden configurar el tiempo de finalización de las sesiones con permisos de lectura/escritura que se establezcan con el producto.

64. Este tiempo de finalización de sesión afecta tanto a la sesión local a través de CLI como a las sesiones remotas a través de la interfaz web (Web UI).
65. Existen dos (2) tiempos de finalización de sesión que pueden ser configurados en el producto:
    - *Session Timeout*: Se trata del tiempo máximo que puede durar una sesión activa sin tener en cuenta la actividad de los usuarios. El tiempo por defecto es de 10 horas.
    - *Idle Timeout*: Se trata del tiempo máximo durante el cual una sesión permanecerá activa mientras no se detecte actividad de usuario. El tiempo por defecto es de 15 minutos.
66. Cuando cualquiera de los dos tiempos de finalización de sesión alcanza su límite, el producto cierra la sesión de administración del usuario.
67. **Los tiempos de sesión deben ser configurados de forma que sean lo más restrictivos posible.**
68. Para configurar el tiempo de finalización de sesión se deben seguir los siguientes pasos:
    a) Acceder a *Authentication > Settings*.
    b) Ir a *Management Sessions.*
    c) Modificar los valores *Session Timeout* e *Idle Timeout*.
    d) Una vez establecidos los valores deseados, hacer clic en *Save* para aplicar los cambios.
69. Los cambios en el tiempo de finalización de sesión aplicarán a las nuevas sesiones de administración que se establezcan en el producto. Para que se apliquen a una sesión activa, se deberá cerrar la sesión y volver a conectarse.
70. Es importante saber que, si se configuran ambos tiempos a 0 segundos, minutos, horas o días, la sesión no expirará nunca y el usuario podrá permanecer autenticado durante un tiempo ilimitado. **Esto no se recomienda.**

5.3 ADMINISTRACIÓN DEL PRODUCTO

5.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

71. El producto podrá ser administrado de forma local a través de CLI y de manera remota a través de su interfaz web HTTPS.
72. Para la administración local del dispositivo, el usuario deberá tener acceso físico al dispositivo y conectarse mediante el puerto serie empleando un *Baud Rate* de 115200 bit/s. La guía de comandos de Fireware [REF1] provee una lista completa de los comandos que se pueden ejecutar a través de esta interfaz.
73. Los usuarios también podrán administrar el dispositivo a través de la interfaz web utilizando el protocolo HTTPS. Al acceder a través de la interfaz web, los usuarios

deberán autenticarse mediante sus credenciales (usuario y contraseña), lo que les dará acceso a la web de administración. Los permisos que tendrá cada usuario dentro de esa web dependerán del rol de usuario que tengan asignado.

74. Una vez el dispositivo se ha configurado en su modo CSfC, tal y como se indica en la sección 5.1 HABILITACIÓN DEL MODO CSFC, **se restringirá el uso de las interfaces de administración del TOE, de forma que solo se podrá acceder al mismo utilizando su interfaz web o su puerto serie. El protocolo SSH quedará deshabilitado.**

75. De igual forma, la habilitación del modo CSfC dejará el producto configurado de tal manera que se use el protocolo TLS 1.2 para las conexiones realizadas a través de su página web. En caso de querer activar el uso de TLS 1.3, se deberán seguir los pasos indicados en la sección 5.1 HABILITACIÓN DEL MODO CSFC para tal propósito.

5.3.2 MENSAJE DE AVISO Y CONSENTIMIENTO

76. Antes del establecimiento de una sesión, **se debe configurar el producto para que muestre un mensaje de aviso sobre las restricciones de uso de la conexión** (*Logon Disclaimer*). Los usuarios deberán aceptar dicho mensaje, previo al establecimiento de la conexión.

77. La habilitación de dicho *banner* se hará desde la interfaz web (Web UI). Los pasos a seguir son:

    a) Ir a *System > Logon Disclaimer*.

    b) Seleccionar la opción *Enable Logon Disclaimer*.

    c) En el campo *Page Title* se deberá indicar el título de la venta del *Logon Disclaimer*.

    d) En el campo *Specify a Disclaimer message* se deberá incluir el texto del mensaje de aviso y consentimiento.

    e) Opcionalmente se puede añadir un **logo** al mensaje mostrado. Para hacerlo se deberá:

        - Seleccionar la opción *Use a custom logo*.
        - Hacer clic en *Upload Logo* y subir la imagen con el logo deseado.

    f) Para finalizar se hará clic en *Save*.

78. Cuando se activa dicho mensaje, los usuarios administradores deberán aceptarlo para poder acceder al producto a través de la Web UI. Este mensaje también aparecerá durante el acceso de usuario a través de la consola CLI.

5.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

79. Tras la habilitación del modo CSfC (ver apartado 5.1 HABILITACIÓN DEL MODO CSFC), el producto queda configurado de manera que solo queda habilitada su interfaz de administración web, así como los servicios necesarios.

80. Al tratarse de un *firewall*, los usuarios administradores podrán habilitar o deshabilitar las diferentes reglas de tráfico del mismo así como sus puertos en función de las necesidades de la red. Esta configuración podrá ser llevada a cabo siguiendo los pasos indicados en la sección 5.12 POLÍTICAS DE CORTAFUEGOS.

5.5 GESTIÓN DE CERTIFICADOS

81. Se recomienda el uso de certificados para la autenticación en las conexiones HTTPS de administradores y pares VPN IPsec.

82. El certificado por defecto que presenta el servidor web es un certificado auto-firmado. **Se deberá modificar dicho certificado y configurar el producto de forma que use un certificado firmado por una CA elegida por el usuario.**

83. Para importar un nuevo certificado empleado para los servicios web del producto se deben seguir los siguientes pasos:

    a) *Generar una CSR*: Para generar una CSR (*Certificate Signing Request*) se debe acceder a través de la interfaz web y navegar a *System > Certificates*. Se deberá hacer clic en *Create CSR*, en *Next* y se seleccionará *General Use*.

    b) Se introducirán los detalles del certificado y se hará clic en *Next*.

    c) Se especificarán los detalles del dominio, incluyendo el *SN, DNS Name e IP address*, que deberán contener los valores adecuados para la implementación del producto (Dirección IP y nombre de dominio correctos) y se hará clic en *Next*.

    d) En la ventana de selección de algoritmos se deberá elegir **ECDSA con P-256 o P-384, o RSA con una longitud de 3072 o 4096 bits** y se seleccionará *Both* en el campo de *Key Usage*.

    e) Tras hacer clic en *Next* aparecerá el CSR, que deberá ser enviado a la autoridad certificadora para ser firmado. Se hará clic en *Finish*.

84. Una vez se reciba el certificado firmado por parte de la CA, este debe ser importado en el sistema junto al certificado de la CA y cualquier otra CA Intermedia. Para ello se seguirán los siguientes pasos:

    a) Se accederá a *System > Certificates* y se hará clic en *Import Certificate*.

    b) Se hará clic en *Next*, se seleccionará *General Use* y se volverá a hacer clic en *Next*.

    c) En la opción *Import Type* se seleccionará *Base64(PEM) certificate*, que deberá ser el formato en el que se introduzcan los certificados.

    d) En la siguiente ventana se importará el certificado seleccionándolo mediante el botón *Browse* o copiándolo en la casilla disponible. Finalmente se hará clic en *Finish*.

85. El proceso de importado de certificados se repetirá para importar el certificado de la CA, de cualquier CA Intermedia y finalmente, del certificado final del dispositivo.

El orden en el que deben importarse los certificados será ese mismo (CA > CA Intermedia > certificado dispositivo).

86. Una vez importado el certificado, deberá configurarse el producto para que lo use como certificado de la página web. Para ello:
    a) Acceder a *System > Certificates*.
    b) Seleccionar la pestaña *Firebox Web Server Certificate*.
    c) En esa sección, marcar la casilla *Third party certificates* y seleccionar el certificado que se acaba de importar de la lista disponible.
    d) Finalmente, hacer clic en *Save*.
87. Tras ello, la sesión de usuario será finalizada automáticamente y la página web presentará el nuevo certificado.
88. Se deberá tener en cuenta que, aquellos certificados que se instalen en el producto y en los clientes, **deben hacer uso de claves RSA o ECDSA de longitud, al menos, 3072 bits para RSA**, y **curvas P-256 para ECDSA**. Esto permitirá el cumplimiento de los requisitos establecidos en la guía CCN-STIC-807 [REF3] sobre el uso de algoritmos y funciones criptográficas en sistemas de categoría ALTA del ENS.

5.6 SINCRONIZACIÓN HORARIA

89. El producto utiliza el protocolo NTP para sincronizar el reloj del sistema de forma automática con los servidores NTP seleccionados.
90. Es importante que **los servidores NTP se encuentren correctamente configurados** en el producto, ya que este usa la información del tiempo para marcar los registros de auditoría.
91. Durante la configuración inicial, el usuario introduce la zona horaria en la que se encontrará el dispositivo, que será utilizada por el producto para establecer correctamente el tiempo del sistema. La zona horaria y los servidores NTP pueden ser actualizados en cualquier momento por un usuario con el rol de administrador.

5.6.1 MODIFICACIÓN DE LA ZONA HORARIA

92. Es posible cambiar la zona horaria desde la interfaz web del dispositivo. Para ello, se debe navegar a *System > Information*, donde aparecerá la siguiente ventana:

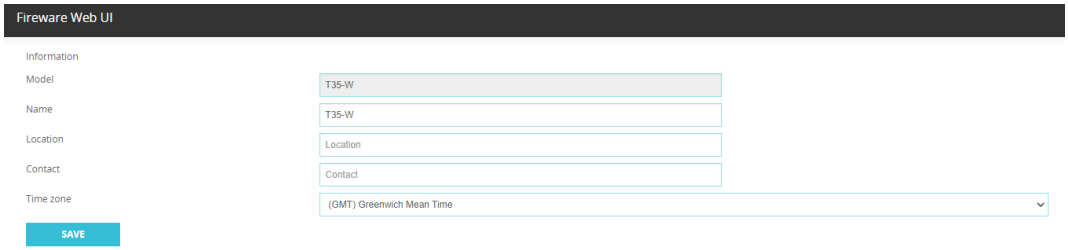

Ilustración 3 - Modificación de la Zona Horaria.

93. En dicha ventana, se debe seleccionar la zona horaria deseada en la lista disponible para la variable *Time Zone*. Una vez seleccionada la zona correcta se hará clic en *Save* y la nueva zona horaria habrá quedado establecida.

5.6.2 CONFIGURACIÓN DE LOS SERVIDORES NTP

94. Los usuarios con el rol de administrador pueden cambiar las opciones de los servidores NTP en cualquier momento.

95. Para ello, se debe acceder al producto a través de su interfaz web y navegar a *System > NTP*.

96. En la nueva ventana se podrán eliminar los servidores NTP existentes marcando la casilla que se encuentra al lado de su nombre y seleccionando la opción *Remove*.

97. Será posible añadir un nuevo servidor NTP seleccionando la opción *Add*. Una vez seleccionada esta opción, el usuario deberá elegir el tipo de dirección que se usará para el servidor NTP (*Host IP* o *Host Name*) y deberá introducir la dirección IP o el nombre de Host del nuevo servidor:

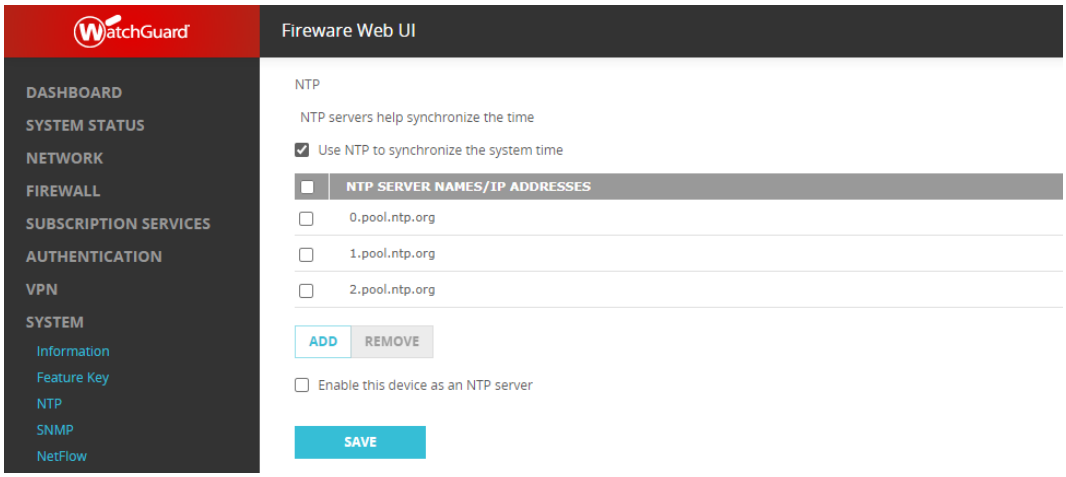

Ilustración 4 - Configuración de los servidores NTP

98. Finalmente se hará clic en *OK* y *Save* y los cambios realizados quedarán guardados.

5.6.3 ACTUALIZACIÓN MANUAL DE LA HORA

99. Si la hora del sistema difiere por más de 1000 segundos con la obtenida mediante un servidor NTP, el producto no actualizará la hora del sistema. En este caso, es posible configurar la hora del sistema de forma manual, de manera que esa diferencia de 1000 segundo vuelva a reducirse y el sistema pueda actualizar la hora automáticamente.

100. Para ello, será necesario conectarse al dispositivo a través del puerto de consola utilizando la cuenta de un usuario con permisos de administrador. Una vez se haya accedido a la consola, se podrán utilizar los siguientes comandos para gestionar el tiempo:

- Para ver el tiempo actual: *show clock*

- Para establecer la hora: *clock time hh:mm:ss*
- Para establecer la fecha: *clock date mm/dd/yyyy*

101. Una vez establecida la fecha y la hora, el usuario podrá cerrar la sesión de la consola escribiendo *exit* y el tiempo del sistema habrá quedado modificado.

5.7 AUDITORÍA

102. El producto genera logs de auditoría entre los que se incluyen los eventos relacionados con las reglas de cortafuegos, cambios de configuración y eventos de seguridad del dispositivo.

103. Por defecto, los logs se almacenan de manera local en el almacenamiento interno del dispositivo. Cada vez que un evento genera un mensaje de log, este se almacena en el espacio de almacenamiento del producto.

104. El almacenamiento interno contiene los eventos más recientes que se han producido en el sistema. Cuando el espacio de almacenamiento se llena, el producto borra los eventos más antiguos que tiene almacenados de manera que puedan almacenarse los nuevos logs. Cada vez que el producto reproduce este comportamiento y borra los logs, se genera un evento que se almacena junto al resto de logs.

105. Es por esto que **se recomienda configurar un servidor externo de auditoría para almacenar los logs de forma segura.** Para ello, se puede consultar las instrucciones indicadas en el apartado 5.7.3 ALMACENAMIENTO REMOTO DE LOGS.

5.7.1 REVISIÓN DE LOS LOGS DE AUDITORÍA

106. Para visualizar los logs de auditoría almacenados en el dispositivo se debe acceder a través de sus servicios web y navegar a *Dashboard > Traffic Monitor*.

107. Los botones que aparecen en la parte superior de la ventana permiten filtrar los eventos por su tipología.

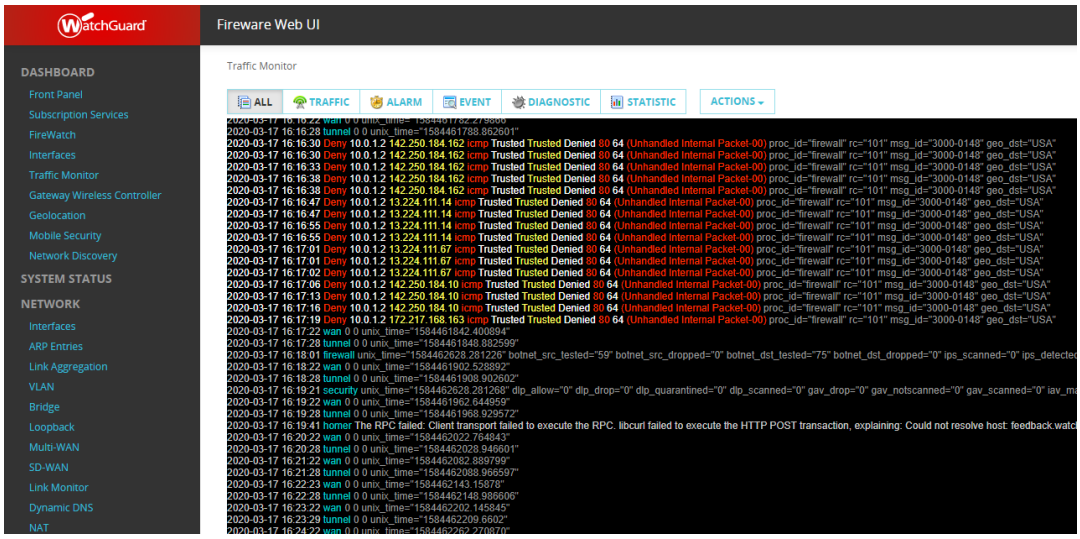

Ilustración 5 - Eventos de Auditoría

5.7.2 CONFIGURACIÓN DE LOS LOGS DE AUDITORÍA

108. Para que el producto genere registros de auditoría, **se deben habilitar las políticas de auditoría en las opciones globales**. En la configuración por defecto, la mayoría de los eventos de auditoría se encuentran habilitados.

5.7.2.1 HABILITACIÓN DE EVENTOS DE LAS POLÍTICAS DE CORTAFUEGOS

109. Las políticas de cortafuegos por defecto tienen habilitados sus mensajes de auditoría. Sin embargo, estos mensajes deben ser habilitados por separado para cada regla de cortafuegos nueva que se introduzca en el dispositivo, en el caso de que se quieran almacenar los eventos asociados a dicha regla.

110. Para ello, se debe acceder a través de los servicios web del dispositivo y navegar a *Firewall > Firewall Policies*. En esta ventana se seleccionará el nombre de la regla de firewall a la que se le quieren habilitar los eventos de auditoría, tras lo cual se abrirá la ventana de edición de la política.

111. En la nueva ventana se deben marcar las casillas *Send a log message* y *Send a log message for reports*. Una vez seleccionadas las casillas, se hará clic en *Save*.

112. En el caso de las políticas de proxy, el procedimiento es parecido. Se debe acceder *a Firewall > Firewall Policies* y seleccionar la política a editar.

113. En la ventana de edición se navegará a la pestaña *Proxy Action*, donde se seleccionará la opción *General* y se marcará la casilla *Enable logging for reports***.** Finalmente se hará clic en *Save*.

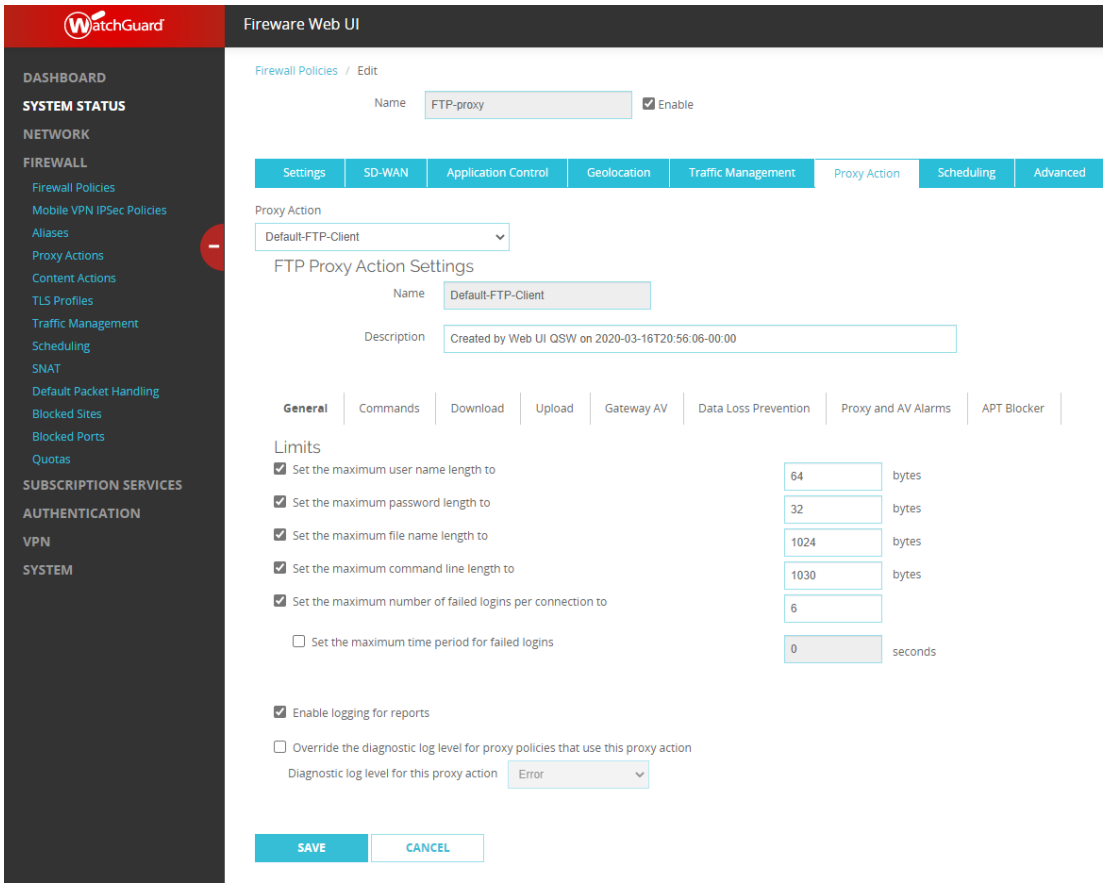

Ilustración 6 - Eventos para las políticas de *proxy*

5.7.2.2 CONFIGURACIÓN GLOBAL DE LAS FUNCIONES DE AUDITORÍA

114. Durante el proceso de configuración se deben habilitar todas las funciones de auditoría disponibles en el sistema.

115. Para ello, se debe acceder al dispositivo a través de su interfaz web y navegar a *System > Logging*. En la nueva ventana se seleccionará la pestaña *Settings*, donde se deberán marcar todas las casillas existentes, habilitando todas las funciones de auditoría del producto. Finalmente se hará clic en el botón *Save*.

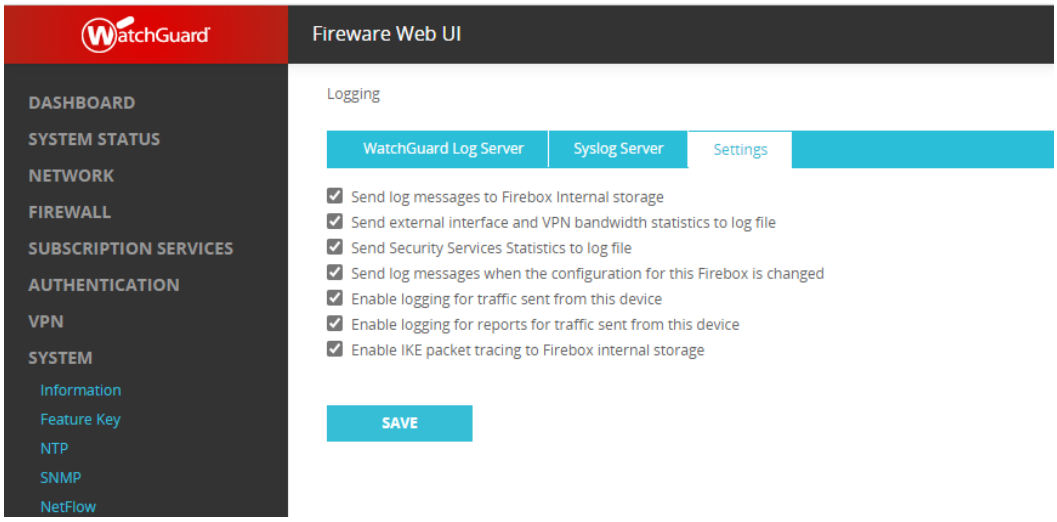

Ilustración 7 - Configuración de la funcionalidad de auditoría

5.7.2.3 CONFIGURACIÓN DEL NIVEL DE DIAGNÓSTICO DE LOS EVENTOS

116. El nivel de diagnóstico de los eventos de auditoría determina el nivel de detalle que se incluye en los archivos de auditoría. Para que el dispositivo genere la cantidad de información necesaria se debe configurar el nivel de diagnóstico con la opción *Debug* para la funcionalidad de administración, configuración y VPN IKE.

117. Para llevar a cabo esta configuración, se debe acceder al dispositivo a través de su interfaz web y navegar a *System > Diagnostic Log*. En la nueva ventana se establecerá el nivel *Debug* para las opciones *Authentication, Management y VPN > IKE*.

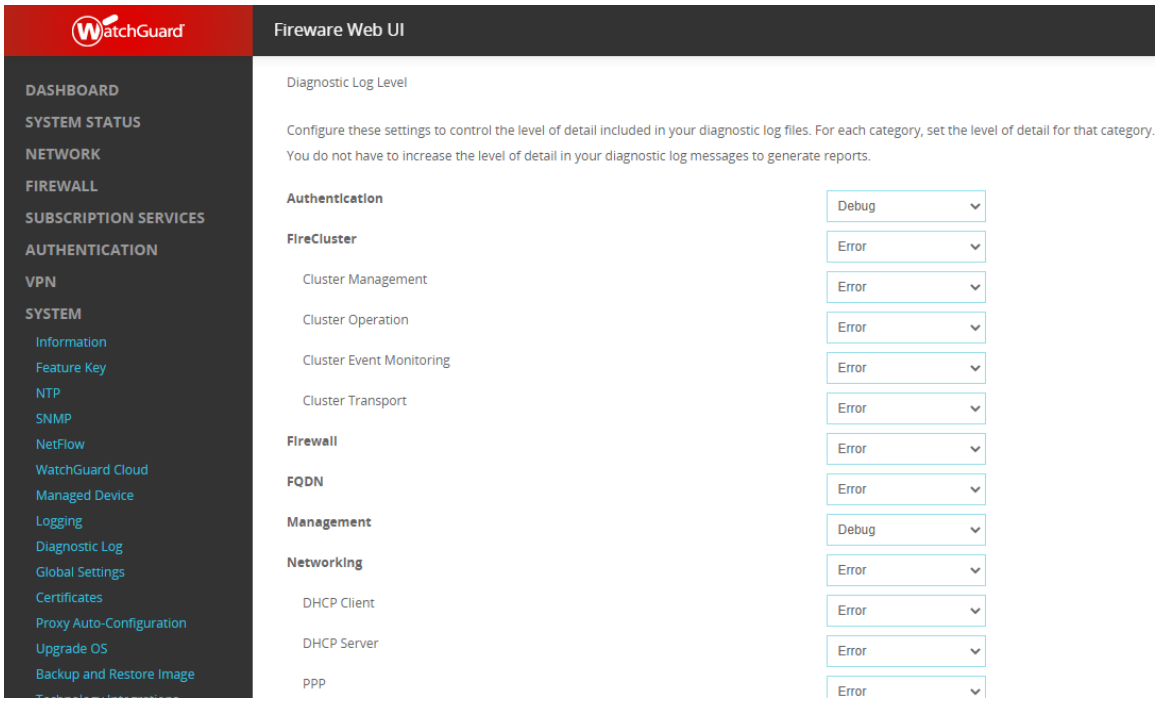

Ilustración 8 - Configuración del Nivel de Diagnóstico.

5.7.3 ALMACENAMIENTO REMOTO DE LOGS

118. El producto permite la configuración del envío de logs a un servidor Syslog externo. En caso de configurarlo, el producto envía de manera inmediata los mensajes de logs generados al servidor Syslog.

119. Es importante tener en cuenta que los logs enviados al servidor Syslog externo no se encuentran cifrados. Para proteger la conexión **se recomienda el uso de un túnel VPN IPsec** que conecte el producto al servidor Syslog. Para mayor información ir al apartado 5.13 VPN IPSEC.

120. Además, los mensajes de apagado de auditoria no se envían al servidor Syslog debido al tiempo de apagado. Estos mensajes estarán disponibles en la Web UI del producto.

121. Para configurar el envío de logs al servidor Syslog externo, se han de seguir los siguientes pasos:

    a) Ir a *System > Logging*.

    b) Hacer clic en *Syslog Server*.

    c) Seleccionar la opción *Send log messages to these syslog servers.*

    d) Hacer clic en *Add*.

    e) Añadir la información relativa al servidor Syslog, como es la dirección IP (*IP Address*) y el puerto (*Port*, que por defecto tiene valor 514).

    f) En la lista de *Log Format* se deberá seleccionar *Syslog*.

    g) Opcionalmente se puede añadir una descripción en *Description.*

    h) Para añadir la fecha y hora de la ocurrencia de un evento se deberá seleccionar la opción de *The time stamp*.

    i) Para incluir el número de serie del dispositivo se deberá seleccionar la opción *The serial number of the device.*

    j) Por último, en el apartado de *Syslog Settings*, se deberá seleccionar la instalación de syslog en la que se almacenarán los mensajes.

122. Finalmente, se guardan todos los cambios pulsando *Save*.

5.8 SERVIDORES DE AUTENTICACIÓN

5.8.1 CONFIGURACIÓN DE DIRECTORIO ACTIVO

123. El producto permite el uso de servidores de Directorio Activo para autenticar a los usuarios del mismo.

124. Para establecer una conexión con un servicio de Directorio Activo se podrá utilizar el asistente de configuración de Directorio Activo desde la página web del producto. Para ello se deberán seguir los siguientes pasos:

a) Desde la web de administración seleccionar la pestaña *Authentication* y se navegará a *Servers > Active Directory*.

b) En dicha sección, hacer clic en *Add*, lo que hará aparecer el asistente de configuración de Directorio Activo. Tras ello, hacer clic en *Next*.

c) En la siguiente pantalla del asistente, introducir el nombre de dominio del Directorio Activo que se quiere emplear en la casilla *Domain Name*. El nombre de dominio deberá incluir el sufijo (e.g. *example.com* en vez de *example*).

d) Hacer clic en *Next*, tras lo que aparecerá el asistente de configuración de servidores de directorio activo.

e) En la casilla *Server Address,* se deberá introducir el nombre de dominio o la dirección IP del Servidor de Directorio Activo.

f) Marcar la casilla *Enable Secure SSL connections to your Active Directory server (LDAPS)* con el objetivo de que la conexión establecida con el servidor de Directorio Activo se encuentre protegida mediante TLS. En caso de que no se marque la casilla los datos se mandarán en forma de hash, pero no estarán protegidos.

g) Hacer clic en *Next* y aparecerá la pantalla final del asistente de configuración, donde se mostrarán los datos configurados.

h) De forma opcional, se podrá marcar la casilla *Edit the Active Directory domain settings after you click Finish*. Si se marca dicha casilla, al hacer clic en *Finish* se mostrarán los ajustes avanzados de configuración de Directorio Activo. En dichos ajustes se podrá configurar el puerto del servidor, añadir servidores de *backup* o modificar los atributos de búsqueda de usuarios del directorio Activo si así fuese necesario en la configuración del servidor de Directorio Activo empleado.

i) Hacer clic en *Finish*.

125. Para agregar un nuevo usuario que se autentique contra el servidor de Directorio Activo se deberán seguir los pasos indicados en la sección 5.2.2 CREACIÓN DE UN NUEVO USUARIO, indicando el servidor de autenticación configurado en la opción *Athentication Server*, siendo necesario que el nombre del nuevo usuario coincida con el usuario que se ha establecido en el servidor de Directorio Activo.

5.9 ACTUALIZACIONES

126. Para la visualización de la versión del dispositivo, se puede realizar a través de la página web de administración, navegando a *Dashboard > Front Panel*. En la parte de la derecha de la página se podrá observar la versión del producto.

127. Para realizar la actualización de la versión con el objetivo de obtener la imagen del *firmware* adecuada o la más actualizada, se deberá acceder a la página *https://software.watchguard.com*. En dicha página, se deberá buscar el modelo del producto en el que se quiere instalar el *firmware* y descargar y descomprimir el archivo *Fireware v12.10 Sysa-dl*.

128. Dicho archivo puede proporcionarse en formato **zip** o **exe**. Si no es posible encontrar la versión correcta del archivo en la página web, se podrá enviar una petición a la dirección de correo CSfC@watchguard.com para que el fabricante la proporcione.

129. Todos los archivos que contienen el *firmware* se encuentran firmados digitalmente mediante el uso del algoritmo **ECDSA** con **SHA-512**. El producto verificará dicha firma antes de iniciar la instalación del *firmware*, no instalándolo en caso de que dicha verificación no sea satisfactoria.

130. Una vez obtenido el *firmware*, se accederá a través de la página web (Web UI) con un usuario administrador y se navegará a *System > Upgrade OS.*

131. Se seleccionará *I have an upgrade file* y se pulsará el botón *Browse* o *Choose File* (dependiendo del navegador), que permitirá elegir el archivo que contiene el firmware.

132. Finalmente, hacer clic en *Upgrade* y esperar a que el dispositivo instale el firmware y se reinicie.

133. Una vez instalado, se volverá a comprobar si la versión del *firmware* es la deseada. En caso de que no lo sea, se tratará de volver a actualizar el dispositivo.

5.10 AUTO-CHEQUEOS

134. Durante el modo CSfC, el producto hace uso del algoritmo de firma digital criptográfica ECDSA con SHA-512 y la curva P-521 para verificar la integridad del producto cada vez que se arranca y antes de cada actualización de *software*. Estos chequeos de integridad aseguran que los archivos del sistema son válidos y no están corruptos.

135. A continuación, se indican los tres (3) diferentes chequeos de integridad realizados por el producto:

- **Chequeos de arranque.** Durante el arranque del producto, se verifica la integridad de los archivos, directorios y dispositivos del producto. En caso de fallo, el producto se apaga.
- Además, durante estos chequeos de arranque se realizan unos **chequeos criptográficos** para verificar el correcto funcionamiento de los algoritmos y funciones criptográficas. Si se da un error, se para el arranque y se muestra el error en la consola.
- **Chequeos en tiempo de ejecución**. Se realizan chequeos de salud de la fuente de ruido aleatorio continuamente durante el tiempo de ejecución para verificar el estado de la fuente de ruido del producto.
- **Chequeos en actualizaciones.** Durante una actualización, al seleccionar un archivo para actualizar el producto, este realiza un chequeo en busca de la firma digital. Si no se puede verificar la firma o si esta no se encuentra presente, no se realiza la actualización.

5.11 *BACKUP*

136. El producto permite la realización de copias de seguridad que sirven para restaurar el estado del dispositivo a un punto anterior.

137. Una imagen de copia de seguridad incluye los siguientes elementos:

- Fichero de configuración.
- Certificados.
- Contraseñas establecidas.
- Configuración de eventos.
- Logo del cliente.
- Número de serie.
- Plataforma y versión.

138. Las copias de seguridad se crean y almacenan de manera local en el almacenamiento del dispositivo y no incluyen el sistema operativo. Estas imágenes se almacenan en formato ".fxi".

139. Para crear una copia de seguridad se deben seguir los siguientes pasos:

a) Desde la interfaz web, navegar a *System > Backup and Restore Image*.

b) Hacer clic en *Create Backup Image*.

c) Escribir el nombre deseado con el que se almacenará la copia de seguridad y hacer clic en *Save*.

140. Tras ello, se generará una nueva copia de seguridad que quedará almacenada en la lista que se puede encontrar en *System > Backup and Restore Image***.**

141. Para restaurar una copia de seguridad, se deberá navegar a esa misma página de administración, se seleccionará el fichero de copia de seguridad que se desee de la lista y se hará clic en *Restore*. Finalmente se confirmará la restauración de la copia haciendo clic en *Yes*.

142. El sistema permite exportar las copias de seguridad, de manera que éstas se puedan almacenar en un dispositivo externo. Para ello, se navegará a *System > Backup and Restore Image*, se seleccionará el fichero de copia de seguridad que se desee de la lista y se hará clic en *Export***.** Esto permitirá al usuario descargar la copia de seguridad y almacenarla en un dispositivo externo.

5.12 POLÍTICAS DE CORTAFUEGOS

143. Las políticas de cortafuegos definen las reglas que utilizará el producto para determinar qué conexiones y contenido serán admitidos como tráfico entrante o saliente a través de las interfaces de red del dispositivo.

144. Cuando se añade una política a la configuración del producto, se añade implícitamente un conjunto de reglas que dictan qué tráfico es permitido o

denegado, basándose en los factores definidos en dichas reglas, como pueden ser el origen y destino del paquete o el protocolo usado en el mismo.

145. A la hora de configurar una política de cortafuegos se definirán las siguientes reglas:

- Configuración de los orígenes y destinos permitidos.
- Habilitar los servicios de seguridad aplicables.
- Configuración de las reglas de filtrado para las acciones de proxy (sólo para políticas de proxy).
- Configuraciones como administración del tráfico, NAT y opciones de auditoría.

5.12.1 POLÍTICAS Y SERVICIOS DE CORTAFUEGOS POR DEFECTO

146. Tras ejecutar el asistente de configuración (ver apartado 4.2.2 ASISTENTE DE CONFIGURACIÓN), el dispositivo queda configurado de forma que se aplican las siguientes reglas:

- Las conexiones a la interfaz de gestión web solo están permitidas desde las redes internas o confiables (*trusted networks*).
- El producto no permite conexiones entrantes desde la red externa (por ejemplo, internet) a la red interna o hacia el propio producto.
- Inspección del tráfico FTP, HTTP y HTTPS saliente (desde la red interna a la red externa) utilizando la configuración por defecto de acciones del *proxy*.
- Se usarán los servicios incluidos dentro de la licencia adquirida por el usuario (*Application Control, WebBlocker, Gateway AntiVirus, Intrusion Prevention, Reputation Enabled Defense, Botnet Detection, Geolocation*, y *APT Blocker security*) con su configuración por defecto.
- Permite el tráfico FTP, ICMP Ping, DNS, TCP y UDP desde las redes confiables hacia las redes externas.

5.12.2 PROTECCIÓN ANTE AMENAZAS POR DEFECTO

147. Tras ejecutar el asistente de instalación, la configuración por defecto del producto tiene habilitada la protección ante amenazas, siendo **capaz de detectar y parar ataques de *SYN flood* y *spoofing*.**

148. Con la configuración por defecto, el dispositivo examina las direcciones IP y puertos de los paquetes y monitoriza su comportamiento en busca de patrones que muestren que la red está en riesgo. Si se detecta un riesgo, el producto puede ser configurado para que el ataque sea detenido automáticamente.

149. La protección ante amenazas por defecto incluye las siguientes configuraciones:

- *Default Packet Handling*: Bloquea actividades consideradas peligrosas, spoofing y ataques de denegación de servicio (ver apartado 5.12.3 MANEJO DE PAQUETES POR DEFECTO).

- *Blocked Sites*: Deniega el tráfico desde las direcciones bloqueadas (ver apartado 5.12.4 SITIOS BLOQUEADOS).
- *Blocked Ports*: Deniega el tráfico entrante desde la red externa a los puertos bloqueados (ver apartado 5.12.4.2 AÑADIR PUERTOS BLOQUEADOS).

5.12.3 MANEJO DE PAQUETES POR DEFECTO

150. Cuando el dispositivo recibe un paquete, examina su origen y destino, direcciones IP y puertos, y monitoriza el flujo de paquetes en búsqueda de comportamientos que puedan comprometer la seguridad de la red. Este proceso de monitorización recibe el nombre de manejo de paquetes por defecto o *default packet handling*.

151. Por defecto, el dispositivo está configurado para bloquear cualquier acción considerada como peligrosa y para detener los ataques de denegación de servicio.

5.12.3.1 CONFIGURACIÓN DEL MANEJO DE PAQUETES POR DEFECTO

152. Para configurar las opciones de manejo de paquetes por defecto, se debe acceder al producto a través de su interfaz web y navegar a *Firewall > Default Packet Handling*.

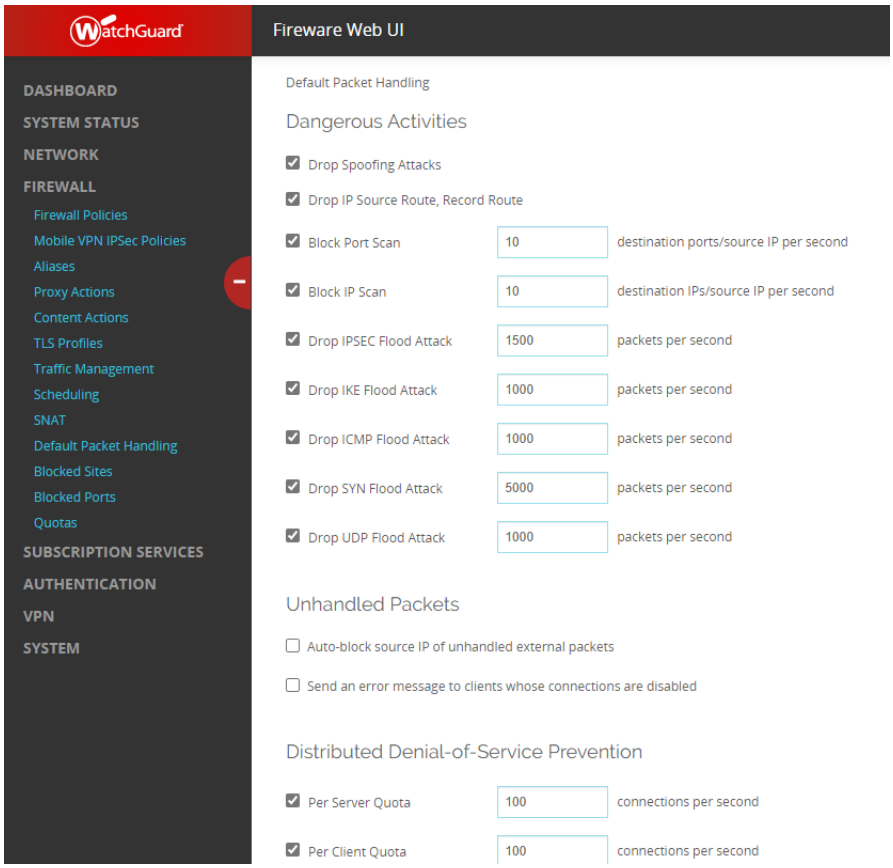

Ilustración 9 - *Default Packet Handling*

153. En dicha interfaz se deberán seleccionar los patrones de tráfico que se quiere que el producto bloquee.

154. Para cambiar los límites que activan el bloqueo de paquetes se debe editar el valor en la casilla que aparece junto al nombre de cada tipo de tráfico.

155. Una vez seleccionados los valores deseados, se debe hacer clic en el botón *Save*.

156. Con el objetivo de prevenir los ataques de denegación de servicio (DoS), el producto permite configurar los límites admitidos de tráfico de paquetes para determinado tipo de tráfico, tal y como se mostró en la configuración previa. Cuando el número de paquetes por segundo recibido por alguna de las interfaces excede el límite establecido, el dispositivo comienza a descartar el tráfico de ese tipo en esa interfaz.

157. El dispositivo no descartará todos los paquetes recibidos inmediatamente tras alcanzar el límite establecido. La siguiente tabla muestra el comportamiento del producto a la hora de descartar paquetes basándose en los límites configurados:

Cantidad de paquetes recibidos	Cantidad de paquetes descartados
Por debajo del límite	No se descartan paquetes
Entre el límite y el doble del límite establecido	El 25% de los paquetes de ese tipo serán descartados
Más del doble del límite establecido	Todos los paquetes de ese tipo se descartan

Tabla 2 Comportamiento de descarte de paquetes según límite configurado

158. Para mayor información sobre los paquetes que son descartados por defecto por el producto, se recomienda ir al apartado "*Packets Dropped By Default*" en la guía *Firebox Common Criteria Deployment Guide* [REF5].

5.12.4 SITIOS BLOQUEADOS

159. Un sitio bloqueado es una dirección IP que no puede establecer una conexión a través del producto. Por defecto, el dispositivo generará un registro de auditoría cada vez que un sitio bloqueado trate de realizar una conexión a la red.

160. Es posible configurar dos (2) tipos diferentes de direcciones IP bloqueadas: permanentes y auto-bloqueadas. También se pueden establecer excepciones de sitios bloqueados.

- *Sitios Auto-Bloqueados.* Si el tráfico cumple una de las políticas o servicios configurados en el cortafuegos con una acción de bloqueo, el producto añadirá automáticamente el sitio a la lista de sitios bloqueados de forma temporal.

  Desde la interfaz web del dispositivo se pueden observar los sitios bloqueados si se navega a *System Status > Blocked Sites*. La lista incluye la razón por la que el sitio fue añadido a la lista y el tiempo de expiración del mismo.

- *Sitios Bloqueados Permanentemente.* Los usuarios con el rol de administrador pueden añadir sitios que serán bloqueados de forma permanente.

- *Excepciones de Sitios Bloqueados.* También es posible añadir excepciones de sitios que no serán bloqueados nunca por el dispositivo. Estas excepciones pueden ser añadidas desde *Firewall > Blocked Sites*. Por defecto, el dispositivo incluye una serie de excepciones productos de *WatchGuard* y servicios suscritos a los que se puede conectar el dispositivo.

5.12.4.1 AÑADIR SITIOS BLOQUEADOS

161. Para editar los sitios bloqueados se debe acceder al dispositivo a través de su interfaz web y navegar a *Firewall > Blocked Sites*.

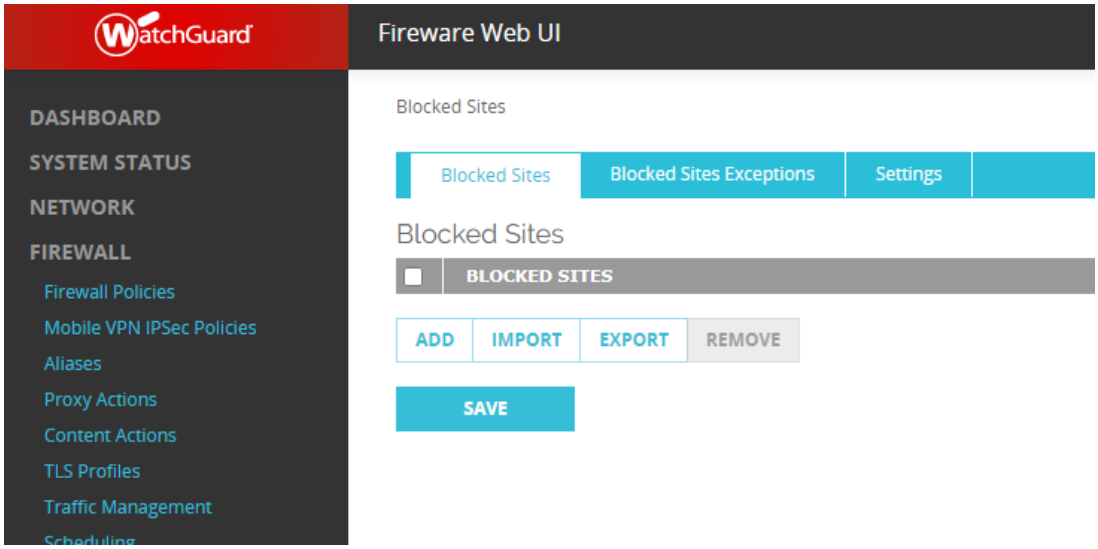

Ilustración 10 - *Blocked Sites*

162. En ese menú de opciones se debe hacer clic en el botón *Add* para añadir un nuevo sitio.

163. En la ventana *Add Sites*, se deberá seleccionar la opción *Choose Type* en función del tipo de sitio que se quiere bloquear, siendo posible elegir entre *Host IPv4, Host IPv6, Host Range IPv4, Network IPv6, Host Range IPv6* y *FQDN*. Una vez seleccionado el tipo, se deberán especificar las direcciones que bloqueadas, que consistirán en una sola dirección IP, un rango de direcciones o un nombre de Host en función del tipo seleccionado.

164. Una vez introducidos los datos de red se hará clic en *OK* y finalmente en *Save*.

5.12.4.2 AÑADIR PUERTOS BLOQUEADOS

165. Los administradores pueden usar la página de administración de puertos bloqueados para añadir puertos a la lista de puertos bloqueados del sistema. El producto denegará el tráfico hacia cualquiera de los puertos bloqueados desde las interfaces externas.

166. Para configurar los puertos bloqueados se debe:

a) Acceder a la página de administración web del producto y navegar a *Firewall > Blocked Ports.*

b) Para añadir un puerto, se introducirá el número del mismo en la casilla inferior y se hará clic en el botón *Add*.

c) Para bloquear automáticamente los sitios que intentan acceder al dispositivo a través de uno de los puertos bloqueados se puede marcar la casilla *Automatically block sites that try to use blocked ports*.

167. Finalmente, se debe hacer clic en la casilla *Save* para guardar los cambios.

5.12.5 CONFIGURACIÓN DE LAS POLÍTICAS DE CORTAFUEGOS

168. El producto utiliza dos (2) categorías diferentes de políticas de filtrado: *packet filters* y *proxies*.

- *Packet Filter Policy*. Una política de filtrado de paquetes examina la cabecera IP de cada paquete de red y su protocolo de transporte. Si la información de la cabecera es legítima y el contenido de la misma cumple una de las políticas que permiten el paso de tráfico, el dispositivo permitirá el paso del paquete. En caso contrario, el paquete será descartado.
- *Proxy Policy.* Una política de *proxy* examina tanto la cabecera IP como el contenido de la capa de aplicación de los paquetes IP y se asegura de que las conexiones y su contenido cumplen los protocolos utilizados. Si la cabecera del paquete es legítima y el contenido del paquete cumple los criterios determinados en la política de *proxy*, entonces el dispositivo permitirá el paso del paquete. Si el contenido del paquete no cumple la política de proxy, este descarta el paquete, o en algunos casos, elimina la parte del paquete que no cumple los criterios.

169. Para cada tipo de política, la plantilla de políticas define los puertos y protocolos a los que la política aplicará.

5.12.5.1 AÑADIR POLÍTICAS DE CORTAFUEGOS

170. La configuración por defecto del producto incluye un conjunto de políticas de cortafuegos y una serie de plantillas de políticas. Cuando se añade una nueva política, se debe elegir una de las plantillas de políticas. La plantilla especificará si se trata de un *Packet Filter* o una *Proxy Policy*, y determinará los puertos y protocolos a los que aplica la política. Después de seleccionar una plantilla de políticas se podrán configurar el resto de propiedades de la política.

171. Tras añadir una política nueva a la configuración se deberán definir reglas como las siguientes:

- Especificar las redes de origen y destino a las que aplicará la política.
- Habilitar los servicios de seguridad.
- Configurar las reglas de filtrado en las acciones de proxy (para las *proxy policies*).

- Configurar propiedades como la administración del tráfico, NAT y propiedades de auditoría.

172. Para añadir una política de *firewall* se debe acceder al dispositivo a través de la interfaz web del mismo y se deben seguir los siguientes pasos:

a) Navegar a *Firewall > Firewall Policies*.

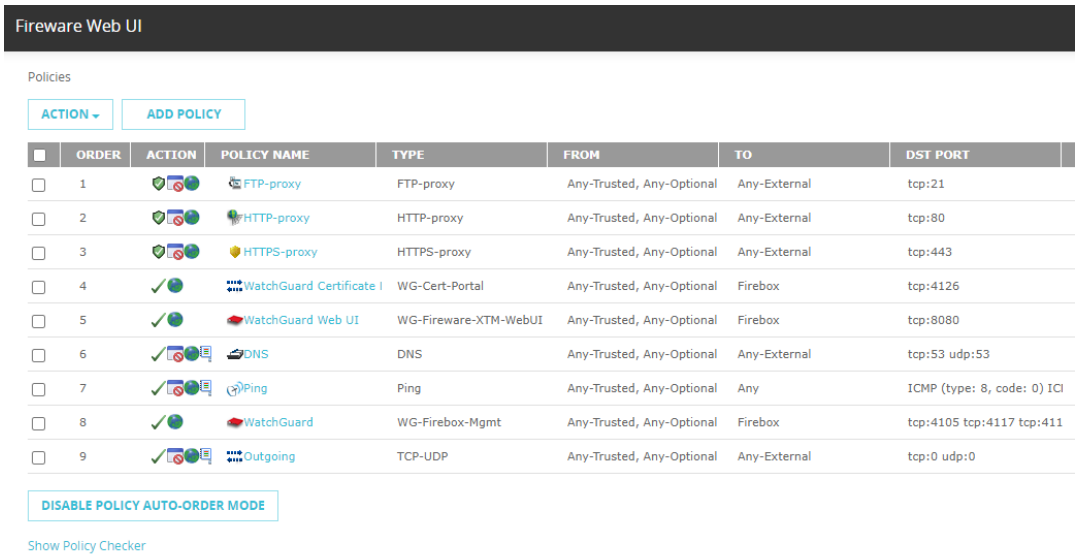

Ilustración 11 - *Firewall Policies*

b) Hacer clic en *Add Policy*.

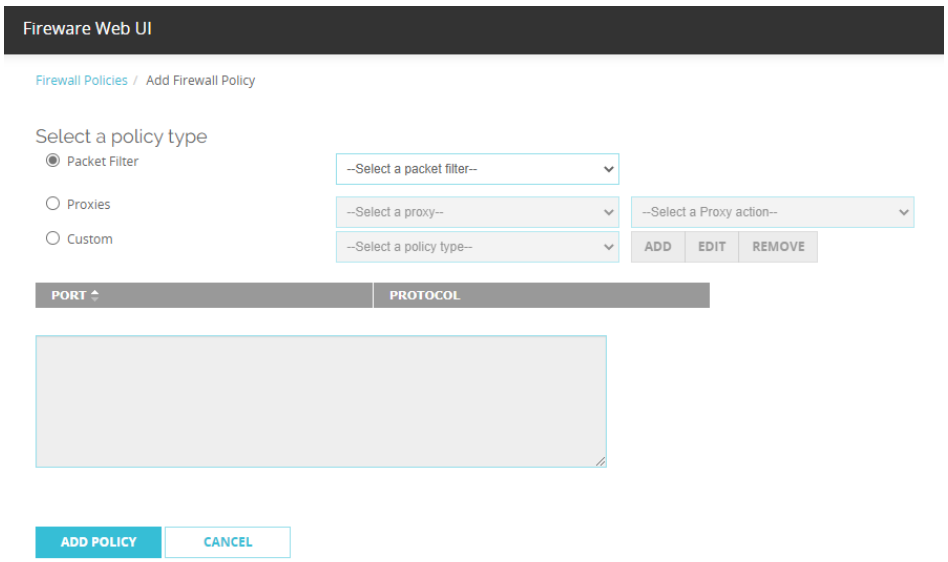

Ilustración 12 - *Add Policy*

c) Seleccionar el tipo de política:

- *Packet Filter.*
- *Proxies.*
- *Custom.*

d) Para un *packet filter*, se deberá seleccionar la plantilla de la lista que aparece adyacente a la opción seleccionada.

e) Para un *proxy*, se debe seleccionar la plantilla de política que aparece en la casilla adyacente y seleccionar una *proxy action* de la segunda lista.

f) Para una política *custom*, se deberá elegir una plantilla de la lista adyacente o hacer clic en *Add* para crear una plantilla a medida.

g) Una vez seleccionada y añadida la política, se hará clic en *Add Policy***.**

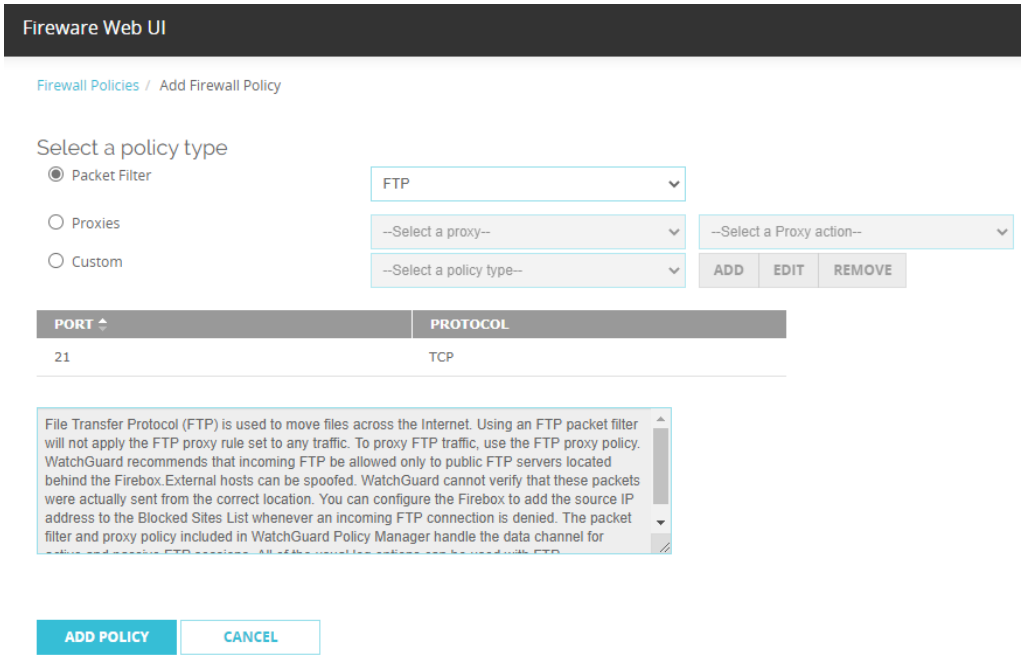

Ilustración 13 - *Policy Template*

h) En la nueva ventana se introducirá el nombre de la política en la casilla *Name* y se configurarán el origen, destino y otras propiedades deseadas, tal y como se definirá en la próxima sección.

i) Adicionalmente, se deberán marcar las casillas *Send a log message* y *Send a log message for reports* (solo se marcará la primera en el caso de un proxy).

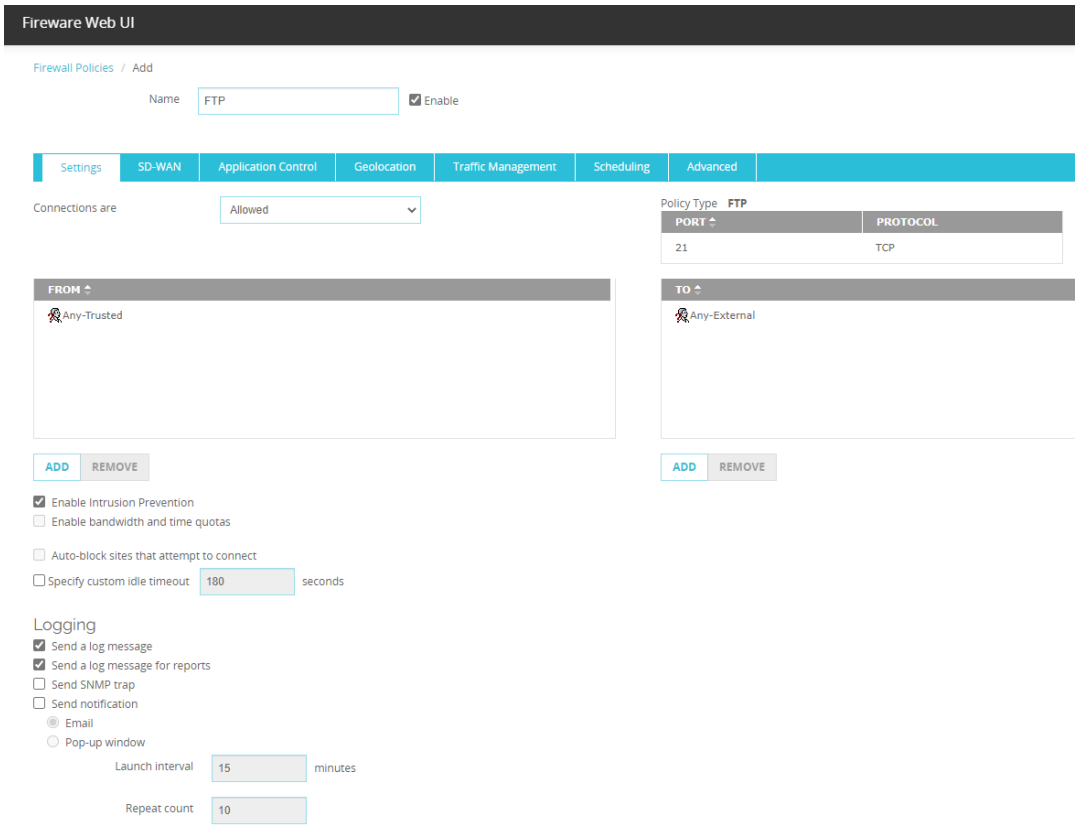

Ilustración 14 - *Policy Configuration*

173. Finalmente, para guardar la nueva política se hará clic en *Save*.

5.12.5.2 CONFIGURACIÓN DE LAS PROPIEDADES DE LAS POLÍTICAS

174. Cada tipo de política tiene una definición por defecto, que consiste en una configuración que es apropiada para la mayoría de organizaciones. Sin embargo, es posible configurar muchas de las opciones por defecto de la política, de forma que se ajusten a las necesidades de cada organización.

175. Para modificar una política, se accederá a *Firewall* > *Firewall Policies*, y se hará clic sobre el nombre de la política que se quiere modificar. De esta manera, se abrirá la página de configuración de dicha política.

176. Desde la pestaña de *Settings* se puede realizar una configuración básica de cada política, como por ejemplo determinar si la política debe denegar o permitir el paso de tráfico o especificar la fuente y destino a los que aplica dicha política. Adicionalmente, es posible configurar NAT estático, cuotas de tráfico y de tiempo o balanceo de carga.

177. La pestaña de *Settings* también muestra el puerto y protocolo a los que aplica la política y una descripción opcional de la misma.

178. La configuración necesaria que se debe aplicar a cada política incluye los siguientes puntos, a los que se puede acceder desde la pestaña de *Settings*:

- *Disposition (Allowed or Denied):* *Disposition* especifica qué acción toma la política con los paquetes que cumplen las reglas de la misma. La lista '*Connections are*' contiene las acciones que pueden ser realizadas por la política y que el usuario debe elegir en función del objetivo de dicha política.

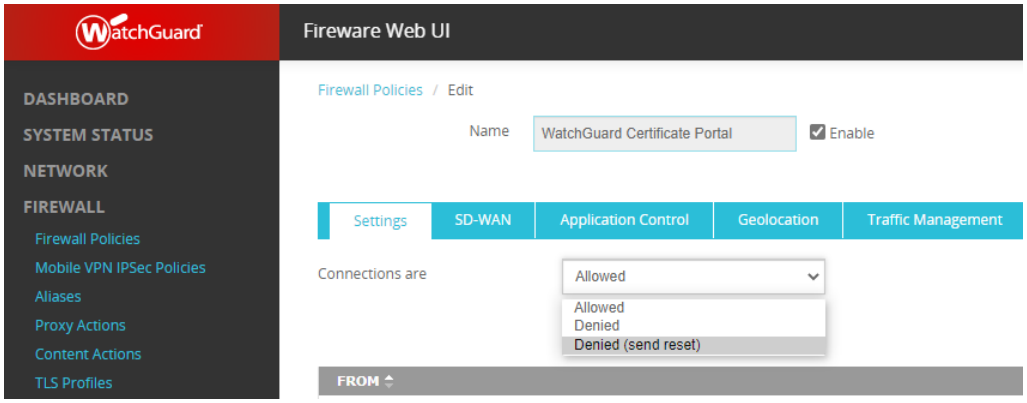

Ilustración 15 – *Disposition*

- Para configurar esta opción, el usuario debe seleccionar una de las siguientes opciones de la lista *Connections are*:
  - *Allowed:* El producto permitirá el paso del tráfico que use esta política si sus características cumplen las reglas establecidas en la política.
  - *Denied:* El producto denegará el tráfico que cumpla las reglas establecidas mediante esta política y no mandará una notificación al dispositivo que generó dicho tráfico. La política podrá añadir automáticamente una dirección IP o red a la lista de sitios bloqueados si intenta establecer una conexión que cumpla esta política.
  - *Denied (Send reset):* El producto denegará el tráfico que cumpla las reglas establecidas mediante esta política y mandará una notificación al dispositivo que generó dicho tráfico indicando que la sesión ha sido rechazada. La política podrá añadir automáticamente una dirección IP o red a la lista de sitios bloqueados si intenta establecer una conexión que cumpla esta política.
- *Source and Destination*: En cada política, se deben especificar los orígenes y destinos de las conexiones a las que aplicará dicha política. Una conexión debe coincidir con ambos, el origen y destino de la política para que la política le sea aplicada.

  En cada política se configura una lista de origen y destino que especifican las direcciones de origen y destino a las que aplicará la política.

  Para configurar las listas de origen y destino se deberá hacer clic en el botón *Add* que se encuentra debajo de las listas *From* (origen) y *To* (destino).

  En la ventana que se abrirá se deberá seleccionar el tipo de miembro que se añadirá a la lista:

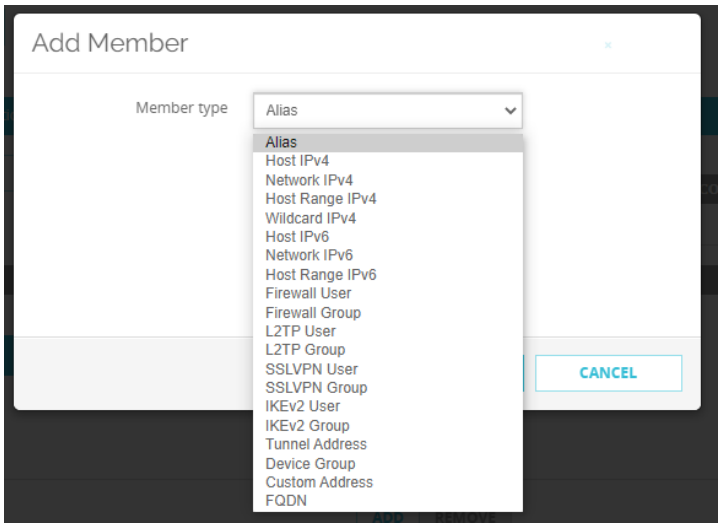

Ilustración 16 - *Member Type*

En función del tipo de miembro seleccionado, se deberá completar la información que lo identificará. Como ejemplo, si se selecciona *Alias*, se nos permitirá elegir entre una lista de miembros que representan a las interfaces internas y externas del dispositivo, en cambio, si se selecciona *Host IPv4* se permitirá introducir una dirección IP que indicará el origen o destino al que aplicará la política.

Para eliminar uno de los miembros de las listas *From* y *To* se debe hacer clic sobre el miembro que se quiere eliminar y seleccionar el botón *Remove*.

- *Ports and protocols*: Los puertos y protocolos a los que aplica una determinada política no pueden ser modificados, ya que están basados en la plantilla seleccionada a la hora de crear dicha política.

  El dispositivo incluye plantillas que cubren la mayor parte de los protocolos y puertos más usados. Sin embargo, existe la posibilidad de crear una política que aplique a un puerto específico si se selecciona el tipo de política *Custom* a la hora de crear la misma, tal y como se explica en la sección 5.12.5.1 AÑADIR POLÍTICAS DE CORTAFUEGOS.

- *Logging*: El producto genera mensajes de auditoría cada vez que aplica una de las reglas de tráfico sobre el tráfico que pasa por el cortafuegos. Para que el producto genere registros de auditoría para el tráfico permitido, se debe habilitar dicha opción en la política de filtrado.

  Para habilitar dicha funcionalidad en una política del tipo *packet filter*, se deben marcar las casillas *Send a log message* y *Send a log message for reports* en las opciones de dicha política.

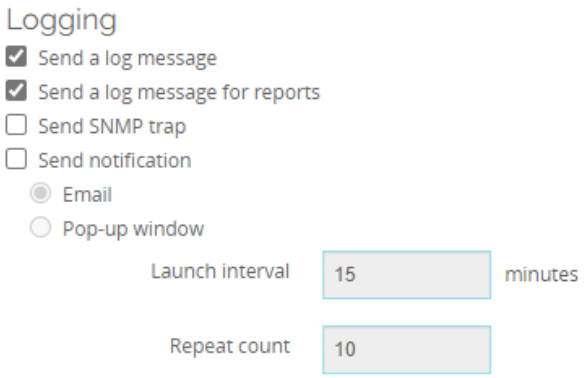

Ilustración 17 - Habilitación de los Eventos de las Políticas.

Para habilitar las funciones de auditoría en una política del tipo *proxy policy*, se debe marcar la casilla *Enable logging for reports* en la ventana *Proxy Action* dentro de las opciones de dicha política.

5.12.6 ORDEN DE PREFERENCIA DE LAS POLÍTICAS

179. La preferencia se refiere al orden en el que el cortafuegos examina el tráfico de red y aplica las políticas que cumple dicho tráfico. El producto emplea la política con máxima preferencia para determinar si el tráfico que cumple dicha política debe ser aceptado o denegado. Cualquier tipo de tráfico que no cumpla ninguna política es marcado como tráfico no manejado y su paso a través del firewall es denegado.

180. Por defecto, las políticas de firewall están configuradas con un orden automático. En este modo, el producto ordena las políticas de más específicas a más generales, basándose en la comparación de los siguientes atributos: tipo de política, puerto y protocolo, origen y destino, *disposition*, horario de aplicabilidad.

181. En la lista de políticas, la columna que indica *Order*, marca el orden de preferencia de las políticas.

182. Las políticas que se encuentran en las posiciones más altas de la lista tienen una preferencia mayor. Cuando el dispositivo recibe un paquete, le aplica la política que cumpla las características del paquete y que se encuentre más alta en la lista.

183. Cuando el modo automático de orden de preferencia está habilitado, si dos políticas son igual de específicas, una política de *proxy* toma preferencia sobre una política de filtrado de paquetes.

184. El orden automático puede ser deshabilitado mediante la ordenación manual de las políticas en la lista de políticas, tal y como se indica en el siguiente apartado.

5.12.6.1 CONFIGURACIÓN MANUAL DEL ORDEN DE PREFERENCIA

185. Para cambiar del modo de orden automático para la ordenación de preferencia de políticas, al orden manual, se deben seguir los siguientes pasos:

a) Será necesario acceder a través de la interfaz web del producto y navegar a *Firewall > Firewall Policies*.

b) En esa ventana se hará clic en *Disable policy Auto-Order mode*.

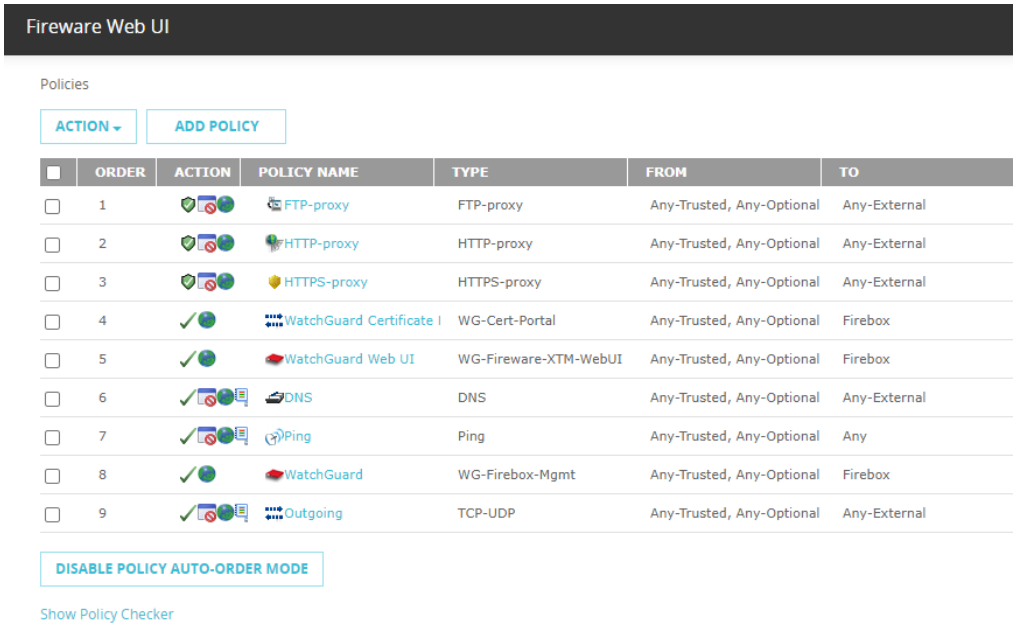

Ilustración 18 - Orden automático de preferencia

c) Se abrirá una ventana de confirmación en la que se deberá seleccionar *Yes*.

d) Para cambiar el orden de las políticas se deberá seleccionar la casilla a la izquierda de cada política y seleccionar los botones *Move Up* o *Move Down* para aumentar o disminuir el orden de preferencia.

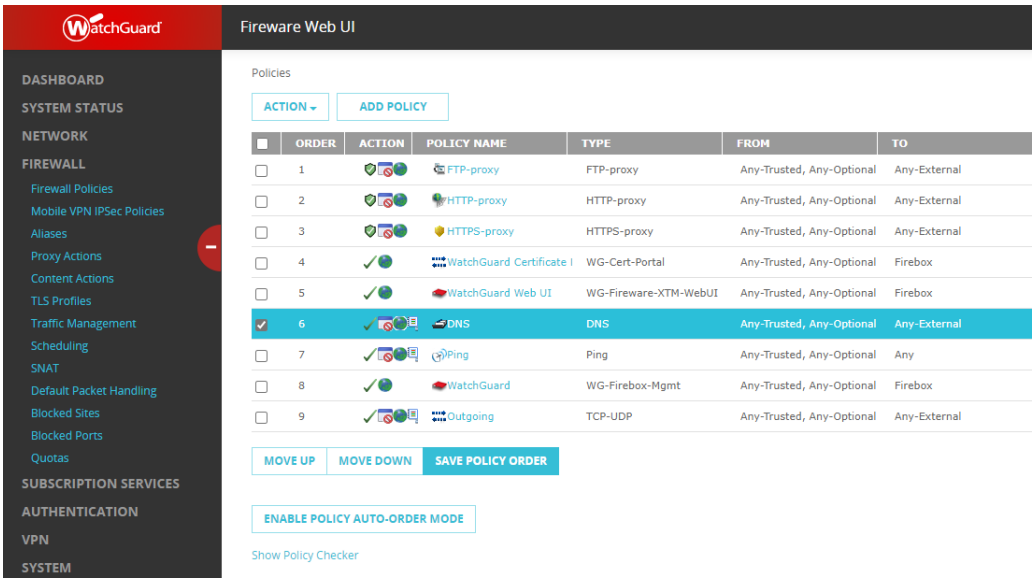

Ilustración 19 - Save Policy Order.

186. Finalmente, se deberá hacer clic en *Save Policy order*.

5.12.7 POLÍTICAS OCULTAS

5.12.7.1 PAQUETES QUE NO CUMPLEN LAS POLÍTICAS ESTABLECIDAS

187. Por defecto, el dispositivo deniega todo el tráfico que no cumple ninguna de las políticas configuradas. Para lograr esto, se usan dos (2) políticas ocultas que tienen un nivel de preferencia menor que cualquiera de las políticas configuradas. Estas dos políticas ocultas son las siguientes:

- *Unhandled Internal Packet:* Esta política deniega todas las conexiones salientes que no están explícitamente permitidas por otra política.
- *Unhandled External Packet*: Esta política deniega todas las conexiones entrantes que no están explícitamente permitidas por otra política.

188. Los nombres de dichas políticas aparecen en algunos de los registros de auditoría cuando deniegan tráfico.

189. Como el producto ya incluye esas políticas, no es necesario incluir ninguna política adicional de denegación de tráfico para el tráfico que no cumple las políticas ya establecidas.

5.12.7.2 SESIONES CON ESTADO

190. *WatchGuard Firebox Next Generation Firewall* es un **cortafuegos con estado**. El dispositivo monitoriza el estado operacional y las características de las conexiones de red permitiendo solo el paso de paquetes que encajan con una sesión activa conocida. El producto no genera un evento de auditoría por cada paquete que coincide con una sesión ya establecida.

5.12.7.3 TRÁFICO GENERADO POR EL PRODUCTO

191. Existe una política oculta adicional, llamada *Any from Firebox*, que permite el tráfico generado por el propio producto. Esta política tiene una preferencia más alta que el resto de políticas existentes, de manera que **el tráfico del propio dispositivo siempre esté permitido**.

5.12.7.4 POLÍTICA IPSEC POR DEFECTO

192. El dispositivo también contiene una política IPSec oculta que permite las conexiones VPN empleando IPSec hacia el propio producto.

193. Esta política oculta se crea cuando se marca la casilla *Enable the built-in IPSec Policy* en la página de configuración global de los servicios VPN. Si se desmarca dicha casilla, la política oculta se eliminará y las conexiones VPN IPSec fallarán.

5.12.8 CONFIGURACIÓN DE POLÍTICAS OBLIGATORIA

194. Con el objetivo de alcanzar una configuración del producto que sea capaz de denegar el tráfico IPv4 e IPv6 inválido será necesario aplicar unas políticas de *firewall* específicas que se describirán a lo largo de esta sección y sus subsecciones.

195. Por tanto, el usuario debe seguir los pasos marcados en estas secciones para alcanzar una configuración segura del producto.

5.12.8.1 DENEGAR EL TRÁFICO RESERVADO PARA USO FUTURO

196. Es necesario añadir unas políticas que denieguen todas las conexiones cuya dirección de origen o destino haya sido definida como "*reserved for future use*" tal y como se especifica en el RFC 5735 para IPv4.

197. Para ello, será necesario añadir dos (2) políticas de *packet filter* con las siguientes características:

- Denegar paquetes desde direcciones IP reservadas:
  - *Plantilla de packet filter: Any.*
  - *Connections are: Denied.*
  - *From: 240.0.0.0/4.*
  - *To: Any.*
  - *Logging: Enabled.*
- Denegar paquetes hacia direcciones IP reservadas:
  - *Plantilla de packet filter: Any.*
  - *Connections are: Denied.*
  - *To: 240.0.0.0/4.*
  - *From: Any.*
  - *Logging: Enabled.*

198. Para configurar estas políticas se deberán seguir los pasos especificados en la sección 5.12.5.1 AÑADIR POLÍTICAS DE CORTAFUEGOS, seleccionando las características de la política especificadas en el punto anterior.

5.12.8.2 DENEGAR EL TRÁFICO DE PROTOCOLOS INVÁLIDOS IPV4

199. Para crear una política que impida el paso de paquetes que usen rangos de protocolos IPV4 inválidos (101-255) será necesario crear una política *custom* siguiendo los pasos que se indican a continuación.

200. Se deberá acceder a través de la interfaz web del producto y navegar a *Firewall > Firewall Policies.* En dicha ventana, se hará clic en *Add Policy* para añadir una nueva política.

201. Se seleccionará una política del tipo *Custom* y se hará clic en *Add*.

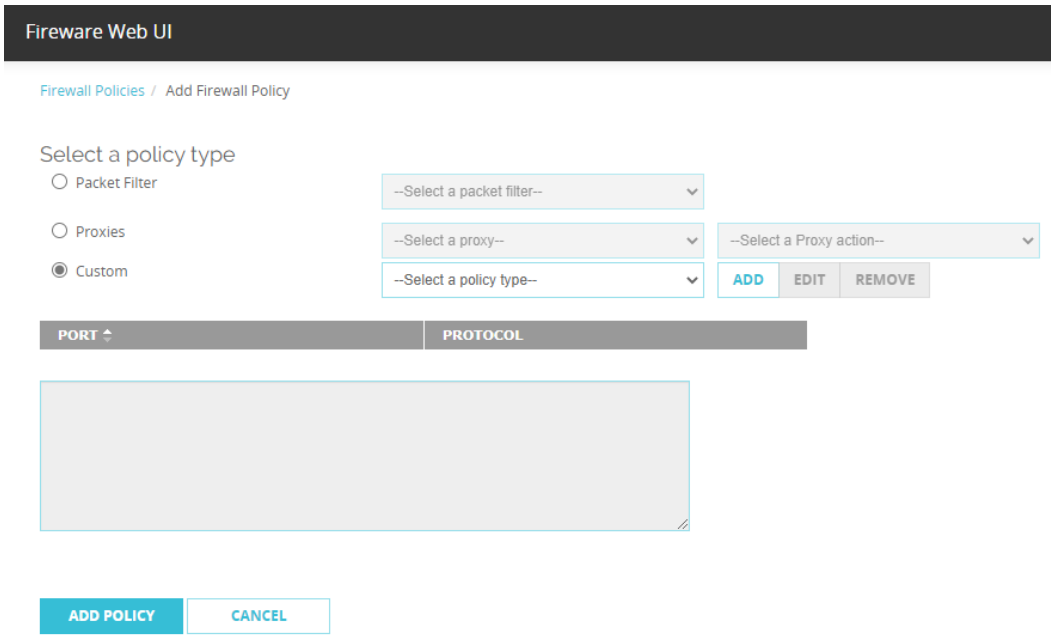

Ilustración 20 - Añadir política personalizada

202. Se debe introducir un nombre y descripción para la nueva política en las casillas *Name* y *Description* respectivamente.

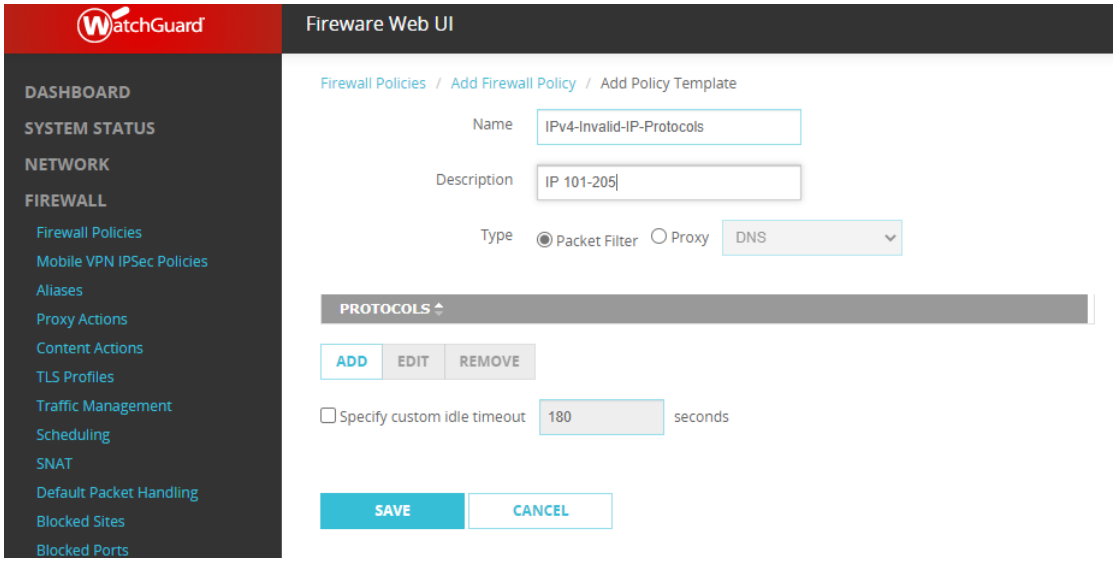

Ilustración 21 - Configuración de la política

203. Se seleccionará el tipo *Packet Filter*.

204. En la lista de protocolos, se deberán añadir los protocolos 101-255. Para ello:

a) Se debe hacer clic en *Add***.**

b) En la lista con el nombre *Protocol* se seleccionará la opción IP.

c) En la casilla *Protocol Number* se introducirá el número del protocolo.

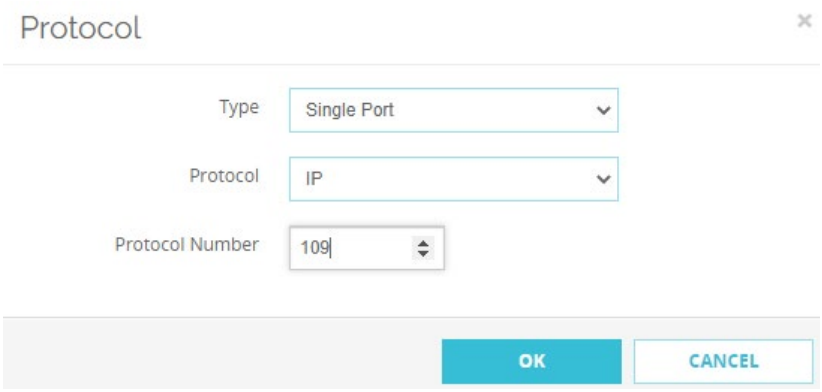

Ilustración 22 - Añadir Número de Protocolo

d) Hacer clic en *OK*.

e) Repetir los pasos anteriores para añadir cada rango de protocolo IP (desde el 101 a 255).

205. Una vez añadido el rango completo de protocolos, se guardará la política haciendo clic en *Save*.

206. Con el objetivo de crear la política que use la plantilla creada, se hará clic en *Add Policy* en la parte inferior de la nueva página que se habrá abierto.

207. La nueva política deberá ser configurada con las siguientes opciones:

- *Connections are: Denied.*
- *From: Network IPv4 address 0.0.0.0/0.*
- *To: Network IPv4 address 0.0.0.0/0.*
- *Logging: Enabled.*

208. Finalmente, se hará clic en *Save* para guardar la nueva política.

5.12.8.3 DENEGAR EL TRÁFICO DE PROTOCOLOS INVÁLIDOS IPV6

209. Para denegar el tráfico de protocolos inválidos IPv6 **se debe añadir una nueva política personalizada para los protocolos 143 a 255**. Los pasos a realizar son muy similares a los indicados en el apartado anterior para denegar el tráfico de protocolos inválidos IPv4.

210. Se deberá acceder a través de la interfaz web del producto y navegar a *Firewall > Firewall Policies*. En dicha ventana, se hará clic en *Add Policy* para añadir una nueva política.

211. Se seleccionará una política del tipo *Custom* y se hará clic en *Add*.

212. Se debe introducir un nombre y descripción para la nueva política en las casillas *Name* y *Description* respectivamente.

213. Se seleccionará el tipo *Packet Filter*.

214. En la lista de protocolos, se deberán añadir los protocolos 143-255. Para ello:

a) Se debe hacer clic en *Add*.

b) En la lista con el nombre *Protocol* se seleccionará la opción IP.

c) En la casilla *Protocol Number* se introducirá el número del protocolo.

d) Se hará clic en *OK*.

e) Se deben repetir los pasos anteriores para añadir cada rango de protocolo IP (desde el 143 a 255).

215. Una vez añadido el rango completo de protocolos se guardará la política haciendo clic en *Save*.

216. Con el objetivo de crear la política que use la plantilla creada, se hará clic en *Add Policy* en la parte inferior de la nueva página que se habrá abierto.

217. La nueva política deberá ser configurada con las siguientes opciones:

- *Connections are: Denied.*
- *From: Network IPv6 ::/0.*
- *To: Network IPv6 ::/0.*
- *Logging: Enabled.*

218. Finalmente, se hará clic en *Save* para guardar la nueva política.

5.13 VPN IPSEC

219. Para crear una conexión segura desde el producto hacia cualquier otro dispositivo existe la posibilidad de configurar una VPN IPSec. En el producto esto se conoce como *Branch Office VPN* (BOVPN).

220. Es posible configurar un *Gateway BOVPN* y añadir uno o más túneles BOVPN que usen dicho *Gateway*. Esta opción permite la configuración de túneles BOVPN entre distintos *WatchGuard Firebox Next Generation Firewall* u otros dispositivos que usen las mismas opciones para el establecimiento del túnel.

221. Cuando se usa esta configuración, el producto siempre enrutará los paquetes a través del túnel BOVPN en el caso de que su origen y destino coincidan con los configurados para el túnel.

222. Por otro lado, como se ha mencionado anteriormente, también se hará uso de un túnel VPN IPsec para proteger la comunicación entre el servidor Syslog externo y el producto.

223. Es importante tener en cuenta que los túneles VPN IPsec **deberán hacer uso del protocolo IKEv2**, y no otra versión, **junto con el uso de certificados**, y no claves precompartidas.

5.13.1 CONFIGURACIÓN DE UN *GATEWAY BOVPN*

224. Un BOVPN Gateway es un punto de conexión para uno o más túneles BOVPN. Para crear un túnel, primero se deben configurar los *gateway* en los dispositivos de origen y destino.

5.13.1.1 AÑADIR UN *GATEWAY*

225. Esta configuración hará que el producto actúe como un *BOVPN Gateway* que podrá establecer túneles con otros *gateways* remotos.

226. Para añadir un *gateway* se debe acceder al producto a través de su interfaz web y seguir los siguientes pasos:

a) Navegar a *VPN > Branch Office VPN*.

b) En la sección *Gateways,* hacer clic en *Add*.

c) Aparecerá una nueva página en la que se deberá introducir el nombre del Gateway en la casilla *Gateway Name* para identificar dicho *gateway*.

d) En la casilla *Address Family* se seleccionará *IPv4 Addresses* o *IPv6 Addresses* en función del tipo de direcciones que vaya a manejar el *gateway* configurado.

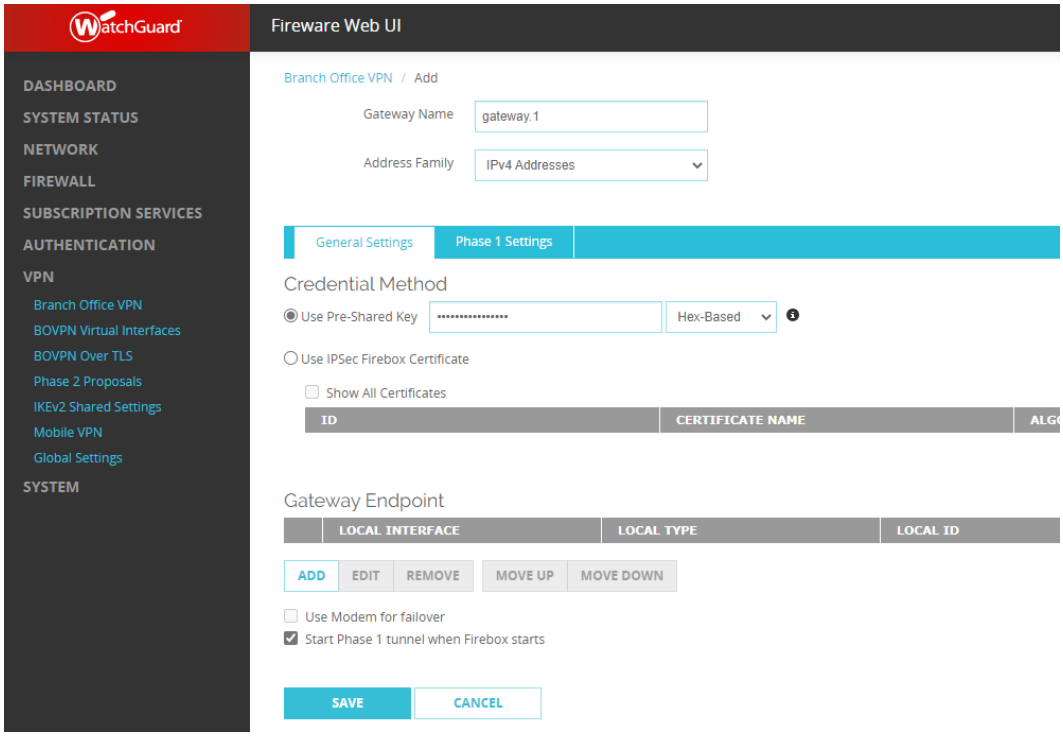

Ilustración 23 - Configuración del Gateway.

227. En el apartado *Credential Method* se seleccionará *Use Pre-Shared Key* o *Use IPSec Firebox Certificate* en función del método de identificación que se empleará en el túnel.

- *Use Pre-Shared Key*: La clave precompartida es una contraseña empleada por dos dispositivos para establecer un túnel que permitirá cifrar y descifrar los datos que pasan por el mismo. Ambos dispositivos deberán ser configurados con la misma clave. Para emplear una clave precompartida se debe seleccionar si la clave introducida será una cadena de caracteres (*string-based*) o una cadena hexadecimal (*hex-based*). Una vez seleccionado el tipo de cadena empleado, se pegará o introducirá manualmente la contraseña.
- *Use IPSec Firebox Certificate*: Si se selecciona esta opción se deberá elegir uno de los certificados actuales que aparezcan en la lista de certificados del producto. Para ver la lista de certificados completa que no incluya un identificador EKU se deberá seleccionar la casilla *Show All Certificates*.

228. Siempre que sea posible, **se recomienda el uso certificados** frente al uso de claves precompartidas. Además, se deberán configurar los *gateways* remotos y locales, tal y como se indicará en las próximas secciones.

5.13.1.2 CONFIGURACIÓN DE LOS *GATEWAYS* REMOTOS Y LOCALES

229. Esta configuración determinará los *gateways* locales y remotos que serán interconectados mediante la BOVPN. La configuración establecerá cómo el producto deberá identificar y comunicarse con los otros puntos de acceso con los que negociará el establecimiento de los túneles. Se debe configurar al menos una pareja de puntos de acceso interconectados cuando se añade un *Gateway BOVPN*.

230. Para configurar los puntos de acceso g*ateway,* se deben seguir los pasos indicados a continuación.

a) Desde la página de administración de los *gateways* descrita en el apartado anterior, se seleccionará el botón *Add* dentro de la sección *Gateway Endpoint*.

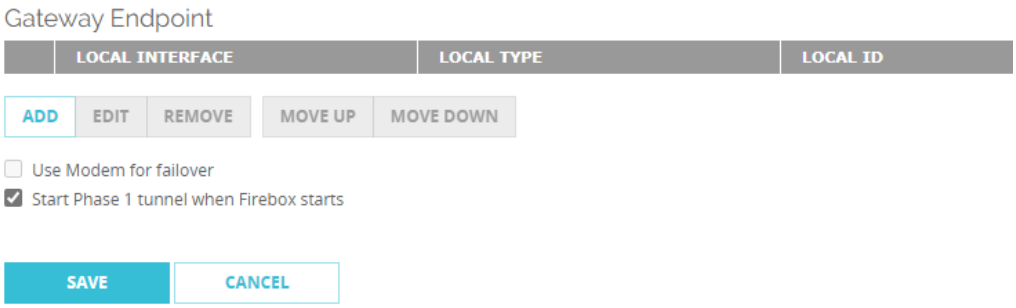

Ilustración 24 – Añadir un *Gateway Endpoint*

b) Se abrirá una nueva ventana en la que se deberá seleccionar la interfaz que tiene la dirección IP pública del sitio al que se le quiere configurar la VPN. Normalmente esta será la interfaz de la red externa del producto. Esta interfaz será seleccionada en la lista *External Interface*.

c) En la opción *Interface IP Address* se seleccionará *Primary Interface IP Address* o se seleccionará una IP secundaria si esta ha sido configurada en la interfaz elegida.

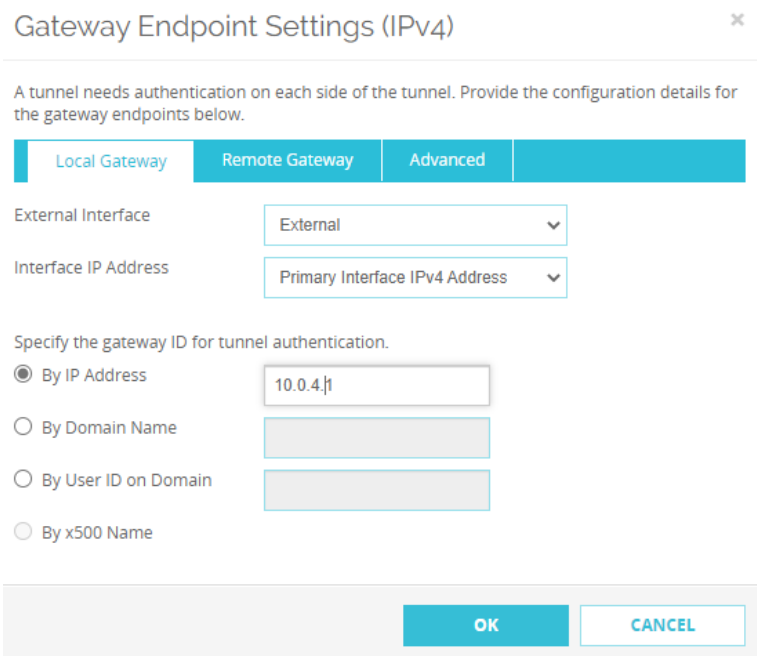

Ilustración 25 - Configuración del Punto de Acceso

d) Se deberá elegir una opción para identificar el *gateway*:

- *By IP address*: Se escribirá la dirección IP primaria de la interfaz del producto seleccionada anteriormente o la secundaria si se ha elegido esta opción.
- *By Domain name*: Se escribirá el nombre de dominio que redirigirá a la dirección IP de la interfaz seleccionada en el punto anterior.
- *By User ID on Domain*: Se escribirá un nombre de dominio con el formato *UserName@DomainName*.
- *By x509 Name*: Esta opción aparecerá marcada automáticamente si se ha seleccionado un certificado como método de autenticación.

e) Para configurar el punto de acceso remoto se seleccionará la pestaña *Remote Gateway*.

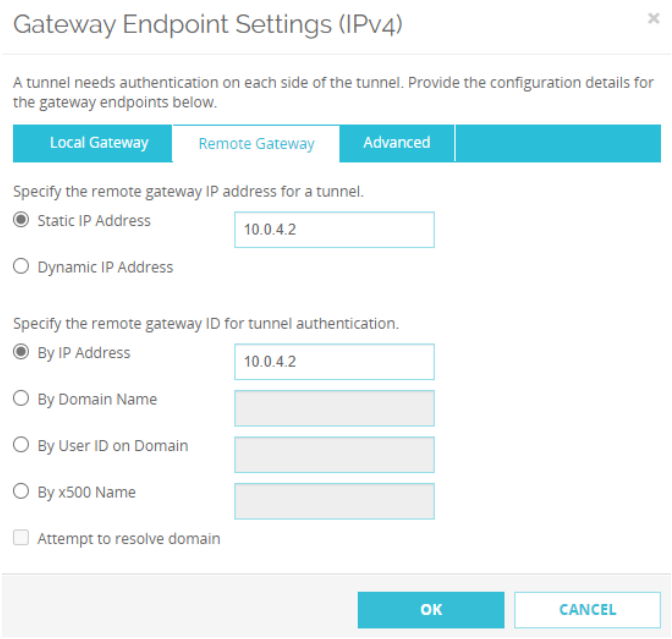

Ilustración 26 - Configuración del Punto de Acceso Remoto

f) En dicha pestaña se determinará el tipo de dirección IP del *Gateway* remoto:

- *Static IP address*: Se debe seleccionar esta opción si el punto de acceso remoto tiene una dirección IP estática. Se deberá escribir en la casilla la dirección IP del punto de acceso.
- *Dynamic IP address*: Se seleccionará esta opción si el dispositivo remoto tiene una dirección IP dinámica.

g) Finalmente, se deberá elegir una opción para identificar el Gateway remoto y se hará clic en **OK**:

- *By IP address*: Se deberá especificar la dirección IP del Gateway remoto.
- *By Domain name*: Se escribirá el nombre de dominio del Gateway remoto.
- *By User ID on Domain*: Se escribirá un nombre de dominio con el formato *UserName@DomainName*.
- *By x509 Name*: Se escribirá el nombre del certificado x509.

h) Para puntos de acceso que empleen IPv4, si el nombre de dominio puede ser resuelto mediante DNS, se marcará la casilla *Attempt to resolve Domain*.

5.13.1.3 CONFIGURACIÓN DE LAS OPCIONES DE FASE 1 DE LA VPN IPSEC

231. Junto con lo indicado anteriormente, se debe configurar la fase 1 del establecimiento del túnel de modo que se emplee **IKEv2**. Para ello, se seguirán los siguientes pasos.

232. Desde la página de administración del *gateway* que se estaba configurando se accederá a la pestaña *Phase 1 Settings*. En dicha pestaña se seleccionará la versión **IKEv2** en la casilla *Version*.

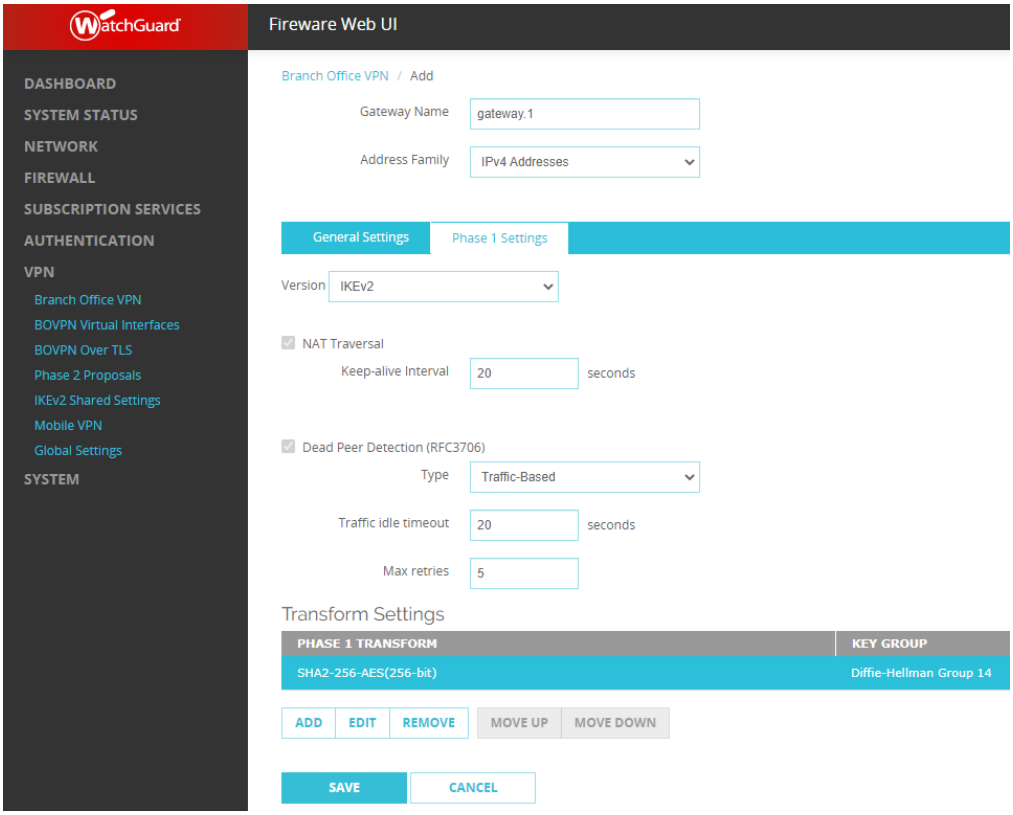

Ilustración 27 - Configuración Fase 1 IPSec

233. Si el *gateway* ha sido configurado con un punto de acceso que tenga una dirección IP dinámica y usa IKEv2 compartido, las opciones de *NAT Traversal* y *Transform Settings* no serán visibles desde esta interfaz. En este caso, esas opciones podrán ser configuradas navegando a *VPN > IKEv2 Shared Settings*.

234. En la opción *Dead Peer Detection*, se debe seleccionar la opción *Traffic-Based* o *Time-Based* en función de las preferencias del usuario. Esta selección determinará cómo el producto detectará que un punto de acceso está desactivado, por la cantidad de tráfico enviado o por el tiempo que se pasa sin enviar tráfico. Las opciones recomendadas para *Dead Peer Detection* son las que vienen marcadas por defecto.

235. Para los *gateways* que no usen opciones compartidas de *IKEv2* se podrán editar las opciones de la transformación IPSec que se emplee en la fase 1 desde esa misma interfaz. Por defecto, las opciones de la transformación especifican el uso de *SHA2, AESC 256* bits en modo *CBC* y el grupo de intercambio de claves *Diffie-Hellman Group 14.*

236. La siguiente sección define cómo configurar y modificar la transformación empleada en la fase 1.

5.13.1.4 AÑADIR UNA TRANSFORMACIÓN DE FASE 1

237. La transformación por defecto cumple todos los requisitos para el nivel medio de la ENS [REF3]. Sin embargo, para categoría ALTA de la ENS **será necesario modificar la transformación, ya que no se acepta el grupo Diffie-Hellman 14.** Además, existe la posibilidad de añadir transformaciones que empleen mecanismos criptográficos más seguros.

238. Para modificar o añadir una transformación a la configuración de un *gateway*, se seleccionará la transformación en la página de configuración del *gateway* dentro de la pestaña de *Phase 1 Settings*.

239. Si el *gateway* ha sido configurado con un punto de acceso que tenga una dirección IP dinámica y usa IKEv2 compartido, las opciones de configuración de la transformación no serán visibles desde esta interfaz. En este caso, esas opciones podrán ser configuradas navegando a *VPN > IKEv2 Shared Settings***.**

240. Para añadir una transformación, se hará clic en el botón *Add*, lo cual abrirá una nueva ventana.

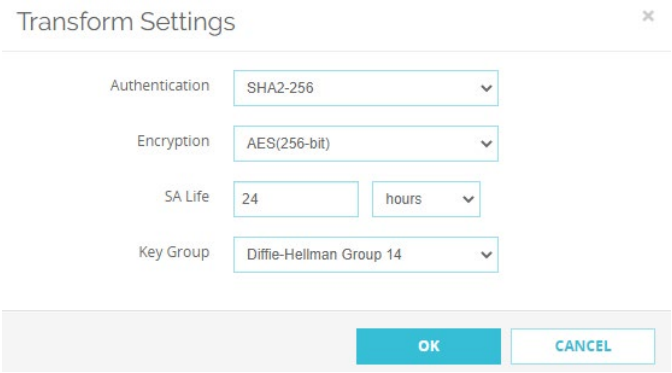

Ilustración 28 - Configuración de la transformación

241. En dicha ventana **se deberá elegir entre *SHA2-256, SHA2-384,* o *SHA2-512*** como método de autenticación, no estando admitido para una configuración segura la elección del algoritmo SHA1.

242. En la opción *Encryption* se elegirá uno de los siguientes métodos: **AES (128-bit), AES (192-bit), AES (256-bit), AES-GCM (128-bit), AES-GCM (256-bit).** No será aceptable para la configuración elegir DES o 3DES como método de cifrado.

243. Para cambiar el tiempo de vida de la asociación de seguridad, se podrá establecer un número en la casilla *SA Life*. El valor debe ser más pequeño de 596523 horas o 35791394 minutos.

244. En la lista de selección asociada a *Key Group*, se deberá elegir uno de los grupos de Diffie Hellman. **Los aceptado son los grupos 19 o 20 y no es aceptable la selección de ningún otro grupo.**

245. Finalmente se hará clic en *OK* para añadir la nueva transformación.

246. Es posible repetir estos pasos para añadir nuevas transformaciones IPSec.

247. Para cambiar la prioridad de las transformaciones simplemente se deberá ordenar su nivel en la lista mediante los botones *Up* y *Down*. Aquella transformación que se encuentre al principio de la lista será la primera en ser usada.

248. Finalmente, se hará clic en *OK* y el Gateway habrá quedado guardado.

5.13.2 CONFIGURACIÓN DE UN TÚNEL BOVPN

249. Una vez se ha definido un *Gateway BOVPN* de manera manual se podrán establecer túneles entre los distintos puntos de acceso.

250. Para establecer un túnel, primero se debe definir dicho túnel y configurar la fase 2 para la negociación de IKEv2. Esta fase establecerá la asociación de seguridad para el cifrado de los paquetes que pasen a través del túnel.

5.13.2.1 AÑADIR UN TÚNEL

251. Para añadir un túnel se deberán seguir los siguientes pasos:

a) Acceder a través de la interfaz web (Web UI) del producto y navegar a *VPN > Branch Office VPN.*

b) En la sección *Tunnels,* hacer clic en *Add*.

c) En la nueva ventana, introducir el nombre del túnel en la casilla *Name*.

d) En la opción *Gateway* se deberá seleccionar el *gateway* que se quiere emplear para establecer el túnel. El *gateway* debe haber sido configurado con anterioridad siguiendo los pasos de esta misma guía.

e) Para añadir el túnel a las políticas *BOVPN-Allow.in* y *BOVPN-Allow.out* se debe seleccionar la casilla *Add this tunnel to the BOVPN-Allow policies*.

f) Estas políticas permiten el paso del tráfico a través del túnel solo si cumple las mismas. Para restringir el tráfico a través del túnel, se puede dejar dicha casilla sin marcar y crear políticas personalizadas para el tráfico que se quiere permitir a través del túnel.

252. Se debe añadir al menos una ruta al túnel, tal y como se describe en la siguiente sección.

5.13.2.2 AÑADIENDO RUTAS AL TÚNEL

253. Las rutas de tráfico del túnel determinan qué tráfico debe ser encapsulado a través del túnel y cual no.

254. Para añadir una ruta al túnel se debe seleccionar la casilla *Add* dentro de la interfaz de configuración del túnel bajo el título *Addresses*. En la nueva ventana, se deben introducir las direcciones local y remota.

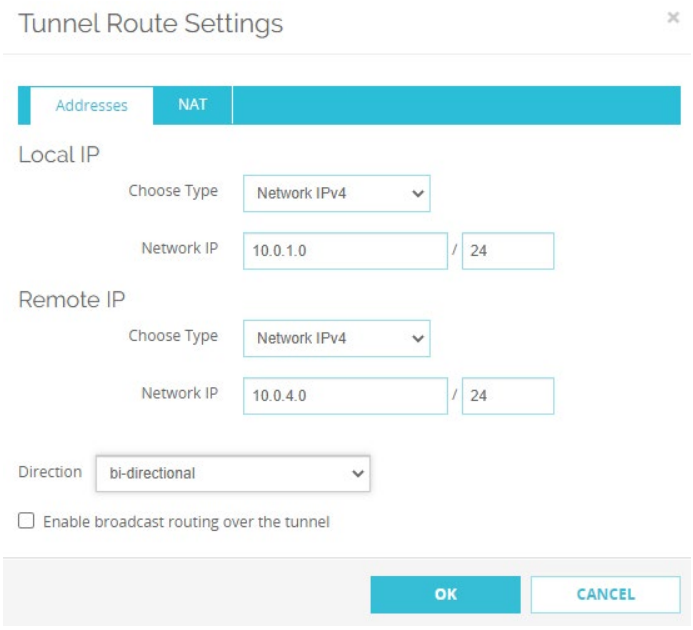

Ilustración 29 - Configuración de rutas del túnel

255. Se seleccionará el tipo de dirección que se va a introducir para establecer la ruta. Se permite seleccionar entre la dirección IP de un *host*, direcciones de una red, un rango de direcciones IP o cualquier dirección. Las direcciones IP seleccionadas en estas listas serán a las que se les aplique la ruta.

256. En las celdas adyacentes se introducirán los valores de direcciones IP de *host*, redes o rangos que se quiere que se enruten a través del túnel.

257. En la opción *Direction* se debe especificar la dirección del túnel. Esta opción determina en qué dirección puede fluir el tráfico a través del túnel. Por defecto, este flujo será bidireccional, fluyendo en ambos sentidos.

258. Si se requiere que se enrute el tráfico de broadcast a través del túnel se debe marcar la casilla *Enable broadcast routing over the tunnel*. En caso contrario la casilla se dejará desmarcada.

259. Finalmente se hará clic en *OK* para guardar la ruta.

5.13.2.3 CONFIGURACIÓN DE LAS OPCIONES DE FASE 2

260. Las opciones de la fase 2 de IKEv2 incluyen las opciones de las asociaciones de seguridad, es decir, define cómo se cifran los paquetes cuando se pasan entre dos (2) puntos de acceso al túnel. La asociación de seguridad (SA) contiene la información necesaria para que cada punto de acceso pueda manejar el tráfico recibido desde otro punto de acceso.

261. Es posible añadir más de una propuesta de fase 2 en la pestaña de opciones de la fase 2. Sin embargo, no se pueden añadir propuestas AH y ESP para el mismo túnel VPN.

262. Las opciones de fase 2 también incluyen la configuración para *Perfect Forward Secrecy* (PFS). PFS proporciona una mayor protección para las claves que son

generadas en cada sesión. Las claves generadas cuando se usa PFS no son derivadas de una clave previa, sino que se genera una nueva clave independiente para cada sesión.

263. Para configurar las opciones de fase 2 se debe acceder a la pestaña *Phase 2 Settings* dentro de la configuración del túnel VPN que se esté configurando.

264. Por defecto, PFS se encuentra habilitado y el grupo Diffie-Hellamn Group 14 se encuentra seleccionado. **Las configuraciones seguras, tal y como indica esta guía, deben contener PFS habilitado y usar los grupos de Diffie Hellman 19 o 20. Cualquier otra configuración no será considerada segura. Se debe evitar la selección de grupo 21 al no estar todavía certificado.**

265. La configuración por defecto del túnel VPN contiene una propuesta por defecto, que aparece en la lista **IPSec Proposals**. Esta propuesta indica que se empleará **ESP**, **AES CBC 256 bits** y **SHA2-256** para la autenticación. Se pueden añadir distintas propuestas a la lista seleccionándolas y haciendo clic en el botón *Add*.

266. Las propuestas empleadas para una configuración segura deben emplear siempre ESP, AES y **un algoritmo de hash que sea al menos SHA2-256** o superior. No se aceptarán como algoritmos seguros el empleo de AH, SHA1, MD5, DES o 3DES.

267. Si no se quiere usar una de las propuestas existentes, existe la posibilidad de crear propuestas personalizadas, tal y como se explica en la siguiente sección.

268. Los algoritmos empleados en la fase 2 no pueden superar en seguridad a los algoritmos seleccionados para la fase 1 configurados durante la configuración del gateway. Si se selecciona un algoritmo que use claves mayores que las empleadas en el algoritmo de fase 1 se mostrará un error y no será posible guardar la configuración.

269. Además, se ha de recordar que los algoritmos empleados deben estar de acuerdo con lo estipulado por la ENS para categoría ALTA en cuanto a seguridad VPN [REF4] y [REF6].

5.13.2.4 AÑADIR UNA NUEVA PROPUESTA DE FASE 2

270. Existen 11 propuestas de fase 2 preconfiguradas en el dispositivo y que no son editables. Para todas ellas el tiempo de expiración de la clave ha sido configurado como 8 horas.

271. Sin embargo, existe la posibilidad de crear nuevas propuestas de fase 2 para combinar los algoritmos disponibles y seleccionar el tiempo de expiración de la clave en base al tiempo y el tráfico si se requiere.

272. Para crear una nueva propuesta de fase 2 se deben seguir los siguientes pasos:

a) Es necesario acceder al dispositivo a través de su interfaz de administración web y navegar a *VPN > Phase 2 Proposals*.

b) En la página de creación de propuestas de fase 2 se hará clic en *Add*, lo que abrirá una nueva ventana.

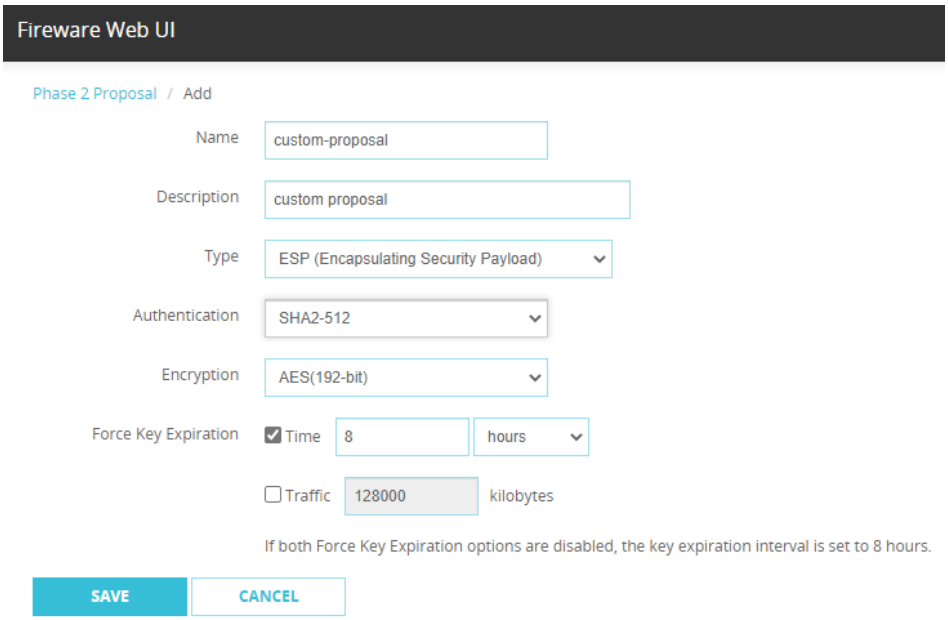

Ilustración 30 - Configuración de nueva propuesta en Fase 2

c) En la casilla *Name* se debe introducir el nombre que se le dará a la nueva propuesta.

d) Opcionalmente, se podrá añadir una descripción de la misma en la casilla *Description*.

e) **Se deberá seleccionar ESP** (*Encapsulating Security Payload*) en la casilla *Type*.

f) Se deberá elegir uno de los algoritmos **SHA2-256, SHA2-384 o SHA2-512** en la casilla *Authentication*. No se debe utilizar otro algoritmo. Esta opción desaparecerá cuando se seleccione AES en modo GCM en la opción de *Encryption*.

g) Se deberá elegir entre **AES (128-bit), AES (192-bit), AES (256-bit), AES-GCM (128-bit), AES-GCM (256-bit)** en la casilla *Encryption*. No será considerado aceptable ningún otro algoritmo de cifrado.

273. Adicionalmente, se puede forzar a los puntos de acceso del túnel a intercambiar una nueva clave tras una cantidad de tiempo o tráfico intercambiado. Para ello se deben marcar las casillas *Time* y/o *Traffic* en la opción *Force Key Expiration* y se deberá especificar la cantidad de tiempo y/o kibibytes tras los cuales se volverá a generar una clave. En caso de que ambas casillas se dejen desmarcadas, se producirá una renovación de la clave cada 8 horas.

5.13.3 AUTENTICACIÓN MEDIANTE CERTIFICADOS PARA BOVPN

274. Por defecto, los *gateways* configurados para BOVPN utilizan un secreto compartido para autenticarse mutuamente. Sin embargo, **se deberá cambiar esta configuración de manera que se utilicen certificados durante la autenticación.**

275. Para emplear un certificado para la autenticación en BOVPN se deben cumplir las siguientes reglas:

- El certificado debe ser un certificado de autenticación para servidor.
- Los certificados de cada punto de acceso deben emplear el mismo algoritmo. Por ejemplo, ambos deben usar RSA o EC. **Si se hace uso del algoritmo RSA, las claves deben tener una longitud de 3072 bits o superior. En el caso de EC, las curvas usadas deberán ser P-256 o superior.**
- El *Subject Alternative Name* (SAN) del certificado no debe contener más de una dirección IP.

5.13.3.1 IMPORTAR UN CERTIFICADO

276. Antes de poder configurar el uso de certificados en BOVPN se deben importar los certificados que se usarán para la autenticación.

277. Cuando se importa un certificado de servidor también se debe importar el certificado de la CA que lo firma y de las CAs intermedias en caso de que existan.

278. Para más información sobre cómo crear e importar un certificado se deben seguir las instrucciones indicadas en la sección 5.5 GESTIÓN DE CERTIFICADOS.

5.13.3.2 CONFIGURAR EL USO DE CERTIFICADOS EN BOVPN

279. Una vez se haya importado un certificado válido, este podrá ser utilizado y asignado en la configuración de BOVPN.

280. Para usar un certificado para la autenticación del túnel BOVPN se debe realizar la siguiente configuración:

a) Aacceder a la página web de gestión del dispositivo y navegar a *VPN > Branch Office VPN.*

b) Para crear un nuevo Gateway, hacer clic en *Add*. También es posible modificar un *gateway* ya existente seleccionándolo y haciendo clic en *Edit*.

c) En la página de configuración, seleccionar *Use IPSec Firebox Certificate.*

d) Seleccionar la casilla *Show All Certificates*.

e) Si el certificado cumple con los requisitos aparecerá en la lista y podrá ser seleccionado como modo de autenticación.

281. Una vez se haya seleccionado el certificado que se usará para autenticar al propio *gateway*, se podrá especificar una CA para verificar el certificado del punto de acceso remoto.

a) Para ello se seleccionará *Edit* tras seleccionar el punto de acceso en la sección *Gateway Endpoints*.

b) En la nueva ventana se hará clic en *Advanced*.

c) En la sección *CA Certificate* se seleccionará la casilla *Specify a CA certificate for remote endpoint verification.*

d) Se seleccionará el certificado de la CA raíz que firmará el certificado del punto de acceso externo en la lista *CA Certificate*.

e) Finalmente, se hará clic en *OK* y *Save*.

5.13.4 AÑADIR POLÍTICAS DE CORTAFUEGOS AL TRÁFICO VPN

282. Las políticas por defecto de BOVPN permiten que todo el tráfico pase a través de los túneles. Sin embargo, es posible crear reglas de cortafuegos que apliquen al tráfico que pasa a través de los túneles IPSec.

283. Para crear una política de cortafuegos que afecte a los túneles VPN se deberán realizar las siguientes acciones:

a) Acceder al dispositivo mediante su interfaz web y se navegará a *Firewall > Policies.*

b) En esa sección, añadir o editar una de las políticas de cortafuegos, tal y como se define en la sección 5.12.5 CONFIGURACIÓN DE LAS POLÍTICAS DE CORTAFUEGOS de esta misma guía.

c) En la ventana de edición de la política, añadir la interfaz del túnel a las listas *From* y *To*. Para ello, hacer clic en el botón *Add* de cada una de las listas, seleccionar *Tunnel Address* en la sección *Member Type* y especificar el túnel al que aplicará dicha política en la opción *Tunnel*.

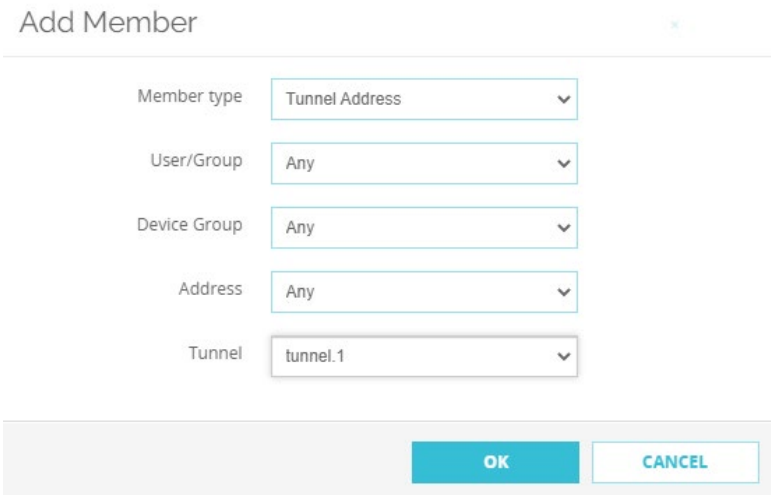

Ilustración 31 - Aplicación de política de cortafuegos a un túnel

d) Finalmente, hacer clic en OK y guardar la nueva política de cortafuegos.

6. FASE DE OPERACIÓN

284. El correcto funcionamiento del producto requiere de características que deben estar presentes en el entorno. Es la responsabilidad del administrador autorizado asegurar que el entorno operacional cumple con los requisitos enumerados a continuación:

a) El producto estará instalado y será mantenido en un entorno físico seguro. Esto incluye un edificio seguro con control de acceso o un entorno móvil controlado por el administrador.

b) El producto no contendrá ninguna aplicación de uso general como compiladores o aplicaciones de usuario.

c) Se realizarán comprobaciones periódicas del *hardware* del dispositivo para asegurar que no ha sido manipulado.

d) Los administradores deben estar correctamente formados en el uso y la correcta operación del producto, así como en las características del entorno seguro en que está presente. Al mismo tiempo, los administradores seguirán las guías e indicaciones presentes.

e) Los administradores se asegurarán de que el producto cuenta con las últimas actualizaciones de *firmware* y *software* para preservar al mismo de amenazas y vulnerabilidades conocidas.

f) Los administradores mantendrán sus credenciales de acceso al producto seguras y protegidas.

g) Los administradores deben eliminar toda la información residual sensible que pudiera quedar resultante de operar con el producto después de terminar la vida útil de este.

h) Los auditores se encargarán de examinar de forma periódica los registros de auditoría buscando eventos específicos relacionados con los cambios de la configuración del sistema y que puedan indicar que este ha sido comprometido.

i) Con el fin de prevenir que los administradores escojan contraseñas inseguras, estas deben cumplir con los siguientes requisitos definidos en 5.2.3 POLÍTICA DE CONTRASEÑAS y seguir las recomendaciones expuestas en la guía CCN-STIC 821, Apéndice V: Normas de Creación y Uso de Contraseñas NP40 [REF2].

j) Además, a la hora de establecer túneles IPsec, se **deberá hacer uso de IKEv2** y no de IKEv1 siguiendo los pasos indicados en el apartado 5.13 VPN IPSEC.

k) No se debe emplear la interfaz de administración SSH del dispositivo durante la operación del mismo. Los usuarios del producto solo deberán usar las interfaces CLI e interfaz web para administrar el producto. Tal como se ha indicado, al activar el modo CSfC se deshabilitará la interfaz.

7. CHECKLIST

285.A continuación, se recoge una tabla con las acciones de configuración que deben realizarse para utilizar el producto de forma segura.

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto	☐	☐	
Instalación en un entorno seguro	☐	☐	
Registro y aplicación de las licencias	☐	☐	
Actualización última versión de *firmware*	☐	☐	
Configuración Servidor NTP	☐	☐	
Configurar el *logging* de todo el tráfico relevante	☐	☐	
Configuración servidor syslog para registros	☐	☐	
Configuración de *backup* y archivado periódico	☐	☐	
Configuración de los Certificados de cliente, maquina, CA's de confianza, etc.	☐	☐	
Configuración de puntos de seguridad a nivel global plasmados en esta guía	☐	☐	
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
Modo de Operación seguro activado (modo CSfC)	☐	☐	
Configurar el *banner* de inicio	☐	☐	
Requisitos mínimos de fortaleza de contraseñas	☐	☐	
Configurar *timeouts* de sesión	☐	☐	
Configurar el bloqueo de las cuentas de usuarios	☐	☐	
Configurar IKE/IPsec	☐	☐	
Creación e instalación de certificados	☐	☐	
Configurar el *logging* de todo el tráfico relevante	☐	☐	

8. REFERENCIAS

REF1 WTG.1, "*Fireware Command Line Interface Reference*", Versión 12.6.4

https://www.watchguard.com/help/docs/fireware/12/en-US/CLI/CLI_Reference_v12_6.pdf

REF2 CCN-STIC 821, Apéndice V: Normas de Creación y Uso de Contraseñas NP40, 2018 CCN-STIC 821, Apéndice V

REF3 CCN-STIC 807 Criptología de empleo en el Esquema Nacional de Seguridad, 2017

CCN-STIC 807 Criptología de empleo en el ENS

REF4 Guía CCN-STIC 836 Seguridad en VPN, 2017 CCN-STIC 836 Seguridad en VPN

REF5 Guía de configuración Common Criteria para Firebox con Fireware 12.10

Firebox Common Criteria Deployment Guide

REF6 Píldora CCN-PYTEC Nº5: Recomendaciones de Seguridad para VPN IPSEC

https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/boletines-pytec/108-pildorapytec-19sep2019-vpn/file

9. ABREVIATURAS

AES	*Advanced Encryption Standard*
AH	*Authentication Header*
BOVPN	*Branch Office VPN*
CA	*Certificate Authority*
CBC	*Cipher Block Chaining*
CCN	*Centro Criptológico Nacional*
CPSTIC	*Catálogo de Productos de Seguridad TIC*
CSR	*Certificate Signing Request*
CRL	*Certificate Revocation List*
DES	*Data Encryption Standard*
DH	*Diffie Hellman Algorithm*
DHCP	*Dynamic Host Configuration Protocol*
DNS	*Domain Name System*
DSS	*Digital Signature Standard*
EC	*Elliptic Curve*
ECDSA	*Elliptic Curve Digital Signature Algorithm*
EKU	*Extended Key Usage*
ENS	Esquema Nacional de Seguridad
ESP	*Encapsulating Security Payload*
FQDN	*Fully Qualified Domain name*
FTP	*File Transport Protocol*
GCM	*Galois/Counter Mode*
HTTP	*Hypertext Transfer Protocol*
HTTPS	*Hypertext Transfer Protocol Secure*
ICMP	*Internet Control Message Protocol*
IKE	*Internet Key Exchange*
IP	*Internet Protocol*
IPsec	*Internet Protocol Security*

NAT	*Network Address Translation*
NTP	*Network Time Protocol*
PEM	*Privacy-Enhanced Mail*
PFS	*Perfect Forward Secrecy*
RSA	*Rivest, Shamir y Adleman Algorithm*
SA	*Security Association*
SAN	*Subject Alternative Name*
SHA	*Secure Hash Algorithm*
SN	*Subject Name*
SPD	*Security Policy Database*
SSH	*Secure Shell Protocol*
STIC	*Seguridad de Tecnologías de Información y Comunicación*
TCP	*Transmission Control Protocol*
TLS	*Transport Layer Security Protocol*
UDP	*User Datagram Protocol*
VPN	*Virtual Private Network*
WAN	*Wide Area Network*
WINS	*Windows Internet Naming Service*

PUBLICACIONES DE DEFENSA

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