centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1409

Procedimiento de Empleo Seguro
Forcepoint NGFW

Julio 2023

MINISTERIO DE DEFENSA

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.01.30 10:05:01 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-24-019-2.
Fecha de Edición: julio 2023

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

ÍNDICE

1. INTRODUCCIÓN

1. La solución Forcepoint NGFW está compuesta por un SMC (*Security Management Center*) encargado de la gestión centralizada de la plataforma, uno o varios Forcepoint NGFW Engines (*firewalls*) y uno o varios Clientes de Gestión.
2. El SMC comprende un Servidor de Gestión (*Management Server*) y un Servidor de Registro (*Log Server*). El Servidor de Gestión es el componente central para la administración del sistema. El Servidor de Registro almacena los registros de auditoría y logs que pueden ser gestionados y compilados en informes. Este Servidor de Registro es capaz, también, de correlar eventos, monitorizar el estado de los NGFW, mostrar estadísticas en tiempo real y reenviar los registros de eventos a servidores remotos de auditoría.
3. La solución se configura y administra a través del Cliente de Gestión, que proporciona una interfaz gráfica (GUI). Este cliente se puede instalar localmente en una estación de trabajo, o iniciarse con un navegador web.
4. Los *NGFW Engines* inspeccionan el tráfico. Permiten funciones de Cortafuegos, VPN, IPS o pueden realizar el rol de cortafuegos de nivel 2.
5. La siguiente figura muestra una visión general de la arquitectura de la solución:

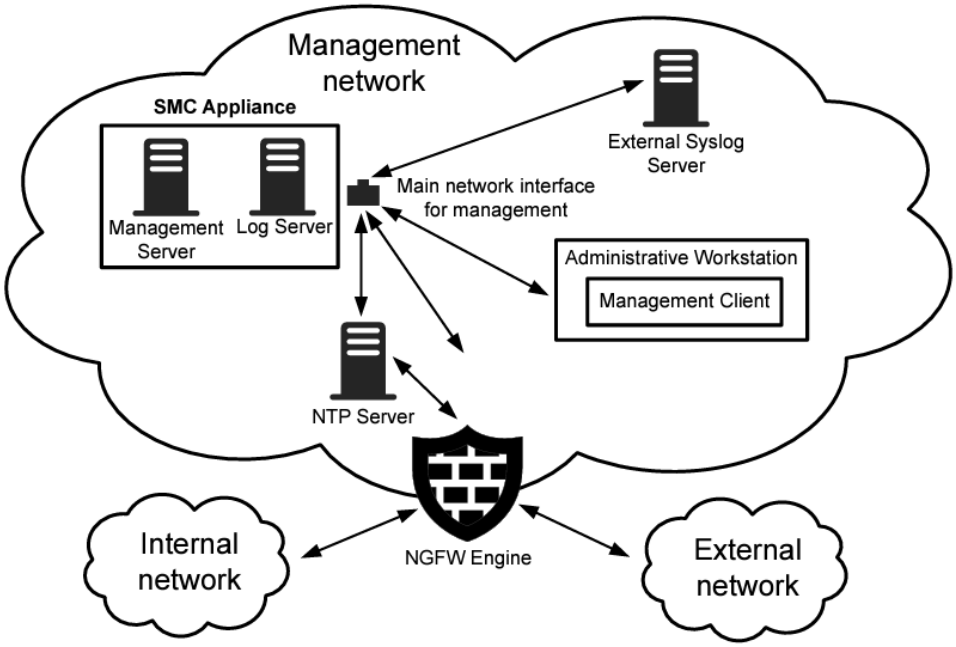

Figura 1 – Visión general de la arquitectura de la solución NGFW

2. OBJETO Y ALCANCE

6. El objeto del presente documento es servir como guía para realizar **una instalación y configuración segura de la solución Forcepoint NGFW**, siguiendo como criterio fundamental el aseguramiento del entorno en el que se despliega.

7. Tanto el SMC (Servidor de Gestión y Servidor de Registro), como los *NGFW Engine*, pueden presentarse en formato *appliance*, o en formato *software*, instalable sobre plataformas compatibles de la organización.

8. La configuración recomendada es el formato *appliance* para ambos componentes (*Security Management Center* y *NGFW Engine*), y el presente documento aplica únicamente a esta configuración:

   a) Forcepoint NGFW Security Management Center (SMC) Appliance **con la versión software 6.10 y:**

      - *OpenSSL 1.1.1 FIPS*
      - *Bouncy Castle FIPS Java API version 1.0.2.1 JCA/JCE provider*
      - *NSS Cryptographic Module version 3.53*

   b) Forcepoint NGFW Engine con la versión software **6.10** y:

      - *OpenSSL 1.1.1 FIPS*
      - *SafeZone FIPS Cryptographic Module 1.2*
      - *Desktop appliance models: N60, N120, N120W, N120WL*
      - *1U appliance models: 2201, 2205, 2210*
      - *2U appliance models: 3410, 3405, 3401*
      - *Forcepoint NGFW Engine as a virtual machine on an ESXi 7.0 server*

9. **Este producto ha sido cualificado e incluido dentro de la familia Cortafuegos de la taxonomía definida por el CCN para el Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC).**

3. ORGANIZACIÓN DEL DOCUMENTO

10. El documento está organizado en varios apartados que cubren los siguientes contenidos:

a) Apartado 4: Recoge los aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.

b) Apartado 5: Recoge los requisitos o recomendaciones asociadas a la fase de despliegue e instalación segura de la solución Forcepoint NGFW.

c) Apartado 6: Describe los requisitos o recomendaciones asociadas a la fase de configuración segura del producto.

d) Apartado 7: Recoge los requisitos o recomendaciones relativas a las tareas de mantenimiento durante la fase de operación y mantenimiento del producto.

e) Apartado 8: Este apartado contiene la documentación a la que se ha hecho referencia a lo largo de este documento.

f) Apartado 9: Este apartado contiene las abreviaturas que han sido empleadas a lo largo de este documento.

4. FASE PREVIA A LA INSTALACIÓN

1.1 ENTREGA SEGURA DEL PRODUCTO

11. A continuación, se **enumeran los pasos que se deben seguir tras la recepción del producto *hardware*:**

a) Una vez recibido el *hardware*, debe examinarse minuciosamente para confirmar que no haya sido manipulado, verificando que esté sellado con cinta y correctamente embalado.

b) En el embalaje en el que se entrega el dispositivo debe estar impreso el logotipo de Forcepoint.

c) Verificar que en el embalaje se incluye una etiqueta blanca codificada para transportes a prueba de manipulaciones. Esta etiqueta incluye el número de producto, el número de serie y otros datos relacionados con el contenido de la caja.

d) Verificar que el paquete ha sido enviado por el proveedor esperado del equipo (Forcepoint / distribuidor autorizado por Forcepoint).

e) Inspeccionar la unidad una vez se haya desembalado. Comprobar que el número de serie del dispositivo coincide con el número de serie que aparece en la factura.

f) Si alguna de las comprobaciones anteriores no es satisfactoria, el usuario deberá ponerse en contacto con el proveedor del equipo (Forcepoint / distribuidor autorizado por Forcepoint).

12. A continuación, se enumeran **los pasos a seguir tras la recepción del producto software**:

a) Si se ha adquirido una suscripción virtual, es necesario que el usuario cree una cuenta en el Portal de Soporte de Forcepoint (*https://support.forcepoint.com*) para poder acceder a la descarga de software y documentación correspondiente.

b) Se debe comprobar la firma SHA-2 para la verificación de integridad tras la descarga del producto. Se debe obtener el hash SHA-2 y comprobar que coincide con el indicado en el área de descarga. Para ello, se puede emplear el comando "*sha256sum <fichero_instalacion>*". La comprobación del hash SHA-256 también puede llevarse a cabo empleando herramientas de terceros.

1.2 ENTORNO DE INSTALACIÓN SEGURO

13. **Se debe instalar el *SMC Appliance* en un Centro de Proceso de Datos (CPD)** que deberá contar con un sistema de control de acceso limitado y restringido al conjunto de personas expresamente autorizadas.

1.3 REGISTRO Y LICENCIAS

14. El *SMC Appliance* y los *NGFW Engine* en formato *appliance* se entregan con el *software* necesario preinstalado, por lo que no es necesario descargar ningún fichero de instalación adicional.

15. Para la operación del sistema se requieren licencias para cada componente: Servidor de Gestión, Servidor de Registro y para cada NGFW Engine. Las licencias de cada servidor del

SMC se instalan cuando se arranca el SMC Appliance tras la instalación inicial. La licencia de cada NGFW Engine se instala cuando se inicia la configuración del NGFW Engine.

16. Es posible consultar la información sobre los distintos tipos de licencias en los apartados Licensing Forcepoint NGFW components y Obtain license files de la guía Forcepoint Next Generation Firewall 6.10 Installation Guide [REF2].

1.4 CONSIDERACIONES PREVIAS

17. Los componentes NGFW Engine pueden desempeñar distintos roles dentro del sistema. Cada rol viene representado por un tipo de elemento distinto dentro del SMC. Será necesario, por lo tanto, tener en cuenta qué roles se desea que represente cada NGFW Engine en el sistema antes de iniciar la configuración.
18. Rol de Firewall / VPN. Los elementos del SMC que lo representan son:
    a) *Single Firewall*: elementos que representan un cortafuegos compuesto por un único dispositivo físico.
    b) *Firewall Cluster*: elementos cortafuegos compuestos de 2 a 16 dispositivos físicos, que trabajan juntos como una sola entidad.
    c) *Virtual Firewall*: elementos NGFW Engines virtuales, en el rol Cortafuegos / VPN.
19. Rol IPS. Los elementos del SMC que lo representan son:
    a) *Single IPS*: elementos que representan un IPS compuesto por un único dispositivo físico.
    b) *IPS Cluster*: elementos que combinan de 2 a 16 dispositivos físicos IPS, que trabajan juntos como una sola entidad.
    c) *Virtual IPS*: elementos que son NGFW Engines virtuales, en el rol IPS.
20. *Rol Layer 2 Firewall.* Los elementos del SMC que lo representan son:
    a) *Single Layer 2 Firewall*: elementos que representan un cortafuegos capa 2 compuesto por un único dispositivo físico.
    b) *Layer 2 Firewall Cluster*: elementos que combinan de 2 a 16 dispositivos físicos cortafuegos capa 2 que trabajan juntos como una sola entidad.
    c) *Virtual Layer 2 Firewall*: elementos que son NGFW Engines virtuales, en el rol cortafuegos capa 2.
21. Rol Master NGFW Engine. Los elementos del SMC que los representan son los Master NGFW Engine, y son dispositivos físicos que albergan los NGFW Engine virtuales. Un Master NGFW Engine es un *appliance* físico que proporciona recursos para los Virtual NGFW Engines.
22. Con anterioridad al inicio de la configuración, además del rol que va a desempeñar cada NGFW Engine, debe decidirse la opción de despliegue más adecuada para ese rol:
    a) Los NGFW Engines en el rol de *Firewall / VPN*, pueden desplegarse únicamente con interfaces físicos de capa 3 (*Layer 3 deployment only*) o pueden tener interfaces de capa 2 y de capa 3 (*multi-layer deployment*).
    b) Los NGFW Engines en los roles de *IPS* y de *Layer 2 Firewall*, se pueden desplegar en modo *inline*, permitiendo un control completo sobre el flujo de tráfico y con la capacidad de bloquear cualquier tipo de tráfico. O se pueden desplegar en modo

Capture para únicamente monitorizar el flujo de tráfico, pero pudiendo responder a ciertas amenazas enviando paquetes que resetean las conexiones. En el rol de *Layer 2 Firewall* existe también el modo de despliegue *Passive inline*, que permite que el tráfico atraviese el cortafuegos, y este únicamente registra logs de las conexiones.

23. Para más información sobre los roles y las opciones de despliegue, es posible consultar el capítulo Preparing for installation de la guía Forcepoint Next Generation Firewall 6.10 Installation Guide [REF2].

1.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

24. SMC es el componente de gestión del sistema Forcepoint NGFW, por lo que debe ser instalado en primer lugar y antes de desplegar ningún NGFW Engine.

25. Los componentes del SMC se pueden instalar sobre un hardware compatible de la organización o se puede usar un *all-in-one SMC Appliance* (que es un dispositivo dedicado destinado a la configuración, administración y monitorización de Forcepoint NGFW), que es la configuración recomendada en este documento.

5. FASE DE INSTALACIÓN

26. El SMC *Appliance* proporciona el Servidor de Gestión y el Servidor de Registro pre-instalados. Al arrancar el *appliance*, se lanza el asistente de instalación (*installation wizard*).

27. El proceso de instalación detallado del SMC Appliance y de los NGFW Engines, se encuentra descrito en la guía *Forcepoint Next Generation Firewall Installation Guide* [REF2]. A continuación, se incluyen algunos aspectos destacados que es necesario tener en cuenta:

28. Durante el proceso de instalación se solicitará un nombre de usuario y contraseña para el administrador sin restricción de permisos (*superuser*) con el que se realizarán las tareas iniciales de configuración. **Deberá introducirse una contraseña segura y que cumpla, al menos, los requisitos mínimos establecidos por en la presente guía** (apartado 6.3.2.1 POLÍTICA DE CONTRASEÑAS Y PARÁMETROS DE SESIÓN).

29. **Se debe configurar el modo de operación seguro en el sistema**. Esto se indica con detalle en el apartado 6.1 Modo de operación seguro, y se lleva a cabo durante la instalación de los componentes del sistema mediante la **selección del modo de ejecución FIPS 140-2 mode, y de la fortaleza de cifrado de 256 bits de longitud.**

30. Cuando la instalación esté completa, el SMC Appliance se reinicia. Se empleará un Cliente de Gestión para llevar a cabo la conexión al SMC Appliance (ver apartado 6.3.1.1 CLIENTE DE GESTIÓN) e iniciar la configuración del sistema. Para más información al respecto, se recomienda consultar el Apartado "*Install licenses for NGFW Engines*", de la Guía de Instalación de Forcepoint NGFW [REF2].

31. Los servidores del SMC y los NGFW Engines requieren licencias para su correcta operación. Si las licencias no están presentes, será necesario instalarlas a través del Cliente de Gestión.

32. Una vez se haya completado la instalación y configuración inicial del SMC, se puede proceder al despliegue de los NGFW Engines, lo cual consiste en añadir y configurar los elementos Engine correspondientes en el SMC, y configurar el *software* Forcepoint NGFW Engine en cada dispositivo en que se desee instalar. Para más información acerca del proceso de configuración inicial, se recomienda consultar el apartado "*Initial configuration of Forcepoint NGFW software*", de la Guía del Instalación del producto [REF2].

6. FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

33. **El sistema debe operar en un modo de operación seguro**. Para ello, los pasos son:

    a) Habilitar el modo FIPS en el arranque del SMC Appliance. El SMC Appliance ejecutará una serie de auto-tests de forma automática.

    b) Si los auto-tests del SMC Appliance reportan errores, será necesario resetear el *appliance* a los valores de fábrica.

    c) Instalar el cliente de gestión (*Management Client*) y establecer los valores de los parámetros de seguridad para una configuración segura.

    d) Crear e instalar los *NGFW Engines en FIPS mode*. El NGFW Engine ejecutará una serie de auto-tests.

    e) Si los auto-tests del NGFW Engine reportan errores, será necesario resetear el appliance a los valores de fábrica.

    f) Revisar los registros de auditoría generados.

34. En los siguientes apartados se indican con mayor detalle las etapas para realizar esta configuración segura. Para obtener más información, se puede consultar la guía How to install Forcepoint NGFW in FIPS mode, versión 6.10, revisión B [REF3].

6.1.1 MODO DE OPERACIÓN SEGURO EN EL SMC APPLIANCE

35. **Se debe aplicar también una configuración de seguridad en el SMC Appliance**. Se deberán seguir los siguientes pasos:

    a) Habilitar el modo FIPS en el SMC Appliance

    b) Comprobar los resultados de los auto-tests ejecutados en el SMC Appliance

    c) Instalar el Cliente de Gestión (*Management Client*)

36. La configuración del modo de operación seguro en el SMC Appliance se realiza durante el proceso de instalación del mismo. Tras la introducción de las credenciales del *superuser*, se solicita la configuración de ciertos parámetros de seguridad. Para activar el modo de operación seguro, deberán seleccionarse:

    a) FIPS 140-2 mode.

    b) *256-bit encryption* (fortaleza de cifrado de 256 bits).

37. Se recomienda configurar el interfaz principal de red del SMC Appliance para la gestión de la conexión con NGFW Engine, y utilizar el segundo interfaz de red para la gestión de la conexión con el Cliente de Gestión y con el servidor *Syslog* externo.

38. A continuación, se pueden ver las opciones 256 bit *Security Strength* y FIPS 140-2 dentro del menú gráfico de instalación:

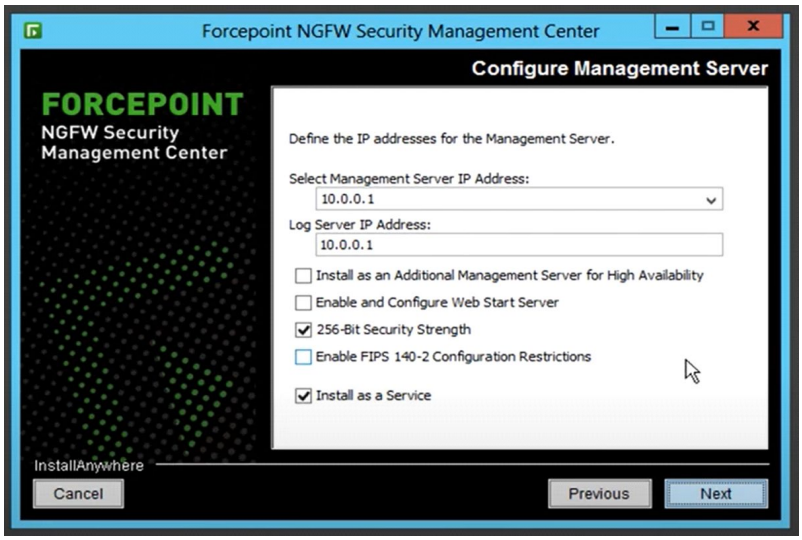

Figura 2 – Selección del Modo FIPS

39. A continuación, se introducen los pasos para **habilitar el Modo FIPS en el SMC Appliance**:

    a) Encender el SMC Appliance.

    b) Aceptar el EULA.

    c) Seleccionar "Comenzar", luego presionar Entrar.

    d) Seleccionar la distribución del teclado para acceder al SMC Appliance en la línea de comandos.

    e) Introducir el nombre de la cuenta de administrador y la contraseña. La cuenta y la contraseña del administrador se utilizan para el acceso de línea de comandos al SMC Appliance y para el acceso al Cliente de Administración (*Management Client*). La cuenta de administrador se crea con permisos sin restricciones (*superusuario*).

        - Introducir el nombre de la cuenta. Este campo distingue entre mayúsculas y minúsculas y está limitado a ocho caracteres.
        - Introducir la contraseña. La contraseña distingue entre mayúsculas y minúsculas. La contraseña debe tener al menos diez caracteres y contener al menos un número.
        - Introducir la contraseña de nuevo.

    f) (Opcional) Configurar una contraseña del gestor de arranque.

    g) Si se desea configurar una contraseña del cargador de arranque (*bootloader*), se deberá ingresar la contraseña del cargador de arranque para editar las opciones que aparecen en el menú del cargador de arranque del SMC Appliance.

        - Presionar la barra espaciadora para configurar una contraseña de cargador de arranque.
        - Introducir la contraseña.
        - Introducir la contraseña de nuevo.

    h) Hacer las selecciones de seguridad.

        - Seleccionar el **modo FIPS**.

- **Seleccionar el cifrado de 256 bits como nivel de seguridad.**

i) Para habilitar la configuración de la interfaz de red, seleccionar "Deshabilitado", luego presionar Entrar.

j) Completar la configuración de la interfaz de red para la interfaz de red principal para la administración.

- Seleccionar "Habilitar interfaz".
- Seleccionar "Primaria".
- Completar los campos de configuración de red para la interfaz.

k) (Opcional) Completar la configuración de la interfaz de red para la interfaz de red secundaria para la administración.

- Seleccionar "Habilitar interfaz".
- Seleccionar "Secundario".
- Completar los campos de configuración de red para la interfaz.

l) Introducir un nombre de host para el servidor de gestión.

m) (Opcional) Ingresar una o más direcciones IPv4 o IPv6 en los campos del servidor DNS. Nota: No se permite la notación CIDR.

n) (Opcional) Si no se desea utilizar NTP, se recomienda desactivarlo en la configuración de NTP.

o) Seleccionar la zona horaria.

p) Configurar la fecha y la hora.

q) Se pedirá que se lleve a cabo la revisión de la configuración.

r) Seleccionar "Confirmar", luego presionar Entrar.

Resultado: Cuando se completa la instalación, el dispositivo SMC se reinicia.

40. El siguiente paso, será testear el SMC Appliance
41. Cuando el SMC Appliance se inicia, se ejecutan automáticamente una serie de auto-tests (*self-tests*): KAT (*Known answer tests*) y PCT (*Pairwise consistency Test*), sobre los algoritmos y funciones criptográficas y sobre la integridad del software.
42. Debe revisarse en la consola el resultado de la ejecución de estos auto-test. Si han sido correctos, se continuará con la configuración del SMC Appliance. Si no lo han sido y el SMC Appliance no se reinicia de forma automática, se debe reiniciar de forma manual. En caso de que tras el reinicio manual el resultado de la ejecución de los tests siga siendo negativo, será necesario resetear el SMC Appliance a los parámetros de fábrica.
43. Si la autocomprobación del módulo criptográfico de *Bouncy Castle* FIPS Java API falla, la aplicación del servidor no se inicia y se muestra un mensaje de error en la consola. El mensaje de error también se envía al Servidor de logs del SMC Appliance.
44. Si falla una autocomprobación de encendido, se muestra un mensaje de error en la consola y el dispositivo se apaga y no se puede acceder de forma remota.
45. Si falla la verificación de integridad del sistema de archivos, se muestra un mensaje de error en la consola y el dispositivo se apaga y no se puede acceder de forma remota.

46. A continuación, se enumeran los siguientes pasos a tener en cuenta:

    a) Si las autocomprobaciones tienen éxito, continuar configurando el SMC Appliance.

    b) Si falla una autocomprobación y el SMC Appliance no se reinicia automáticamente, reiniciarlo manualmente.

    c) Si una autocomprobación sigue fallando, habrá que restablecer el SMC Appliance a la configuración de fábrica. A continuación, se enumeran los pasos a seguir:

        - Conectarse a la línea de comandos del SMC Appliance.
        - Conectar un teclado a un puerto USB y un monitor al puerto VGA, luego presionar Enter.
        - Conectarse a la dirección IP del puerto iDRAC, luego iniciar la consola virtual en la pestaña "Propiedades del servidor".
        - Encender el SMC Appliance, luego, en el menú de inicio, seleccionar VCDROM.
        - Seleccionar "Instalación manual" y comenzar el proceso de instalación.
        - Seleccionar "Instalación nueva", luego presionar Entrar.
        - (Opcional) Resaltar "Borrar disco de forma segura" y luego presionar la barra espaciadora.
        - Seleccionar "Siguiente", luego presionar Entrar.
        - Se pedirá que se revise la configuración.
        - Seleccionar "Confirmar", luego presionar Entrar.
        - Instalar el SMC Appliance en modo compatible con FIPS.

47. El siguiente paso sería llevar a cabo la instalación y configuración segura del Cliente de Gestión (*Management Client*).

48. Para obtener más información sobre la instalación del SMC Appliance en el modo de operación seguro, consultar el capítulo *Installing the SMC Appliance in FIPS mode* de la guía *How to install Forcepoint NGFW in FIPS mode*, versión 6.10, revisión B [REF3].

6.1.2 MODO DE OPERACIÓN SEGURO CLIENTE DE GESTIÓN

49. La configuración del modo de operación seguro en el Cliente de Gestión se realiza durante el proceso de instalación en la estación de trabajo, seleccionando *"Restricted Cryptographic Algorithms Compatible with FIPS 140-2"* como modo de operación.

50. Como paso previo, se introducen una serie de consideraciones previas que habrá que tener en cuenta para el proceso de configuración del Cliente de Gestión en modo seguro:

    a) Instalación del SMC Appliance en Modo FIPS:

        - Si no se cuenta con un SMC Appliance preinstalado, será necesario habilitar las restricciones FIPS en el Servidor de Gestión (*Management Server*), Servidor de logs y el Cliente de Gestión (*Management Client*) cuando los instale.
        - Para obtener instrucciones de instalación detalladas e información sobre los requisitos de hardware para hardware de terceros, se recomienda consultar la Guía de instalación del Firewall de Próxima Generación de Forcepoint y las Notas de la versión del Centro de administración de seguridad NGFW de Forcepoint.

51. Cuando se realice la primera conexión del cliente de gestión con el Servidor de Gestión, se debe verificar la huella (*fingerprint*) mostrada por el Servidor de Gestión.

52. Para obtener más información, consultar el capítulo In*stall the Management Client in FIPS mode* de la guía *How to install Forcepoint NGFW in FIPS mode*, versión 6.10, revisión B [REF3].

6.1.3 MODO DE OPERACIÓN SEGURO NGFW ENGINE

53. La configuración del modo de operación seguro en el NGFW Engine se realiza durante el proceso de configuración de dicho elemento en el SMC, a través del Cliente de Gestión. A la hora de **configurar las propiedades del NGFW Engine se debe seleccionar**:

    a) En Advanced Settings, seleccionar *FIPS-Compatible Operating Mode*.

    b) En Advanced Settings > Log Handling, para *Log Spooling Policy*, seleccione *Stop Traffic* (en el apartado 6.10.2 ALMACENAMIENTO LOCAL de Registros se explica el cometido de este parámetro).

    c) En *Advanced Settings > DoS Protection*, activar *Rate-Based DoS Protection Mode On* y establecer un valor para la opción *Limit for Half-Open TCP Connections*. El límite configurado se aplica por dirección IP de destino. Esta opción se habilita para todo el tráfico permitido en el NGFW Engine, pero se puede anular para cierto tráfico en las opciones de reglas de acceso de la política de cortafuegos.

54. Durante el proceso de instalación del NGFW Engine deberá seleccionarse, también, la opción *FIPS-Compatible Operating Mode* (esta opción habilita el módulo criptográfico FIPS 140-2). Asimismo, durante el proceso de instalación, deberá seleccionarse la opción "*Establecer kernel en modo FIPS*".

55. NGFW Engine contiene OpenSSL FIPS Object Module, NGFW Cryptographic Library, y NGFW Cryptographic Kernel Module. Estos módulos ejecutan los siguientes auto-tests (self-tests) cuando arranca el SMC appliance:

    a) Cryptographic algorithm known answer tests (KAT).

    b) Test de integridad del software usando la función HMAC.

    c) Auto-tests condicionales para la función CTR-DRBG.

    d) *Pair-wise consistency test* (PCT) sobre las claves RSA, DSA y ECDSA generadas.

    e) Chequeo de la integridad de File Systems, usando el *OpenSSL FIPS Object Module* y la función HMAC.

56. **Se recomienda revisar en la consola el resultado de la ejecución de estos auto-tests.** Si han sido correctos, se continuará con la configuración del NGFW Engine. Si no lo han sido y el NGFW Engine no se reinicia de forma automática, será necesario reiniciarlo de forma manual. En caso de que tras el reinicio manual continúe fallando, será necesario resetear el NGFW Engine a los parámetros de fábrica.

57. Para obtener más información sobre la instalación de NGFW Engine en modo de operación seguro, consultar el capítulo Installing the NGFW Engine in FIPS mode de la guía How to install Forcepoint NGFW in FIPS mode, versión 6.10, revisión B [REF3].

6.1.4 LIMITACIONES DEL MODO DE OPERACIÓN SEGURO

58. Cuando el sistema opera en el modo de operación seguro, se aplican algunas de las restricciones al sistema, como las siguientes:

    a) La consola local del NGFW Engine, la consola local del NGFW Engine y el acceso SSH a este no están disponibles.

    b) Los algoritmos criptográficos disponibles y las opciones de configuración en el SMC, están restringidos:

    - **Tamaño de claves RSA mínimo permitido de 2048 bits para la generación de firmas digitales (aunque el tamaño mínimo de clave RSA que se debe utilizar es de 3072 bits, como se indica en apartados posteriores).**
    - **Tamaño de claves ECDSA mínimo de 256 bits** para la generación de firmas digitales. Este es el tamaño mínimo también recomendado.
    - **SHA-1 no puede ser usado para generación de firmas digitales.**

    c) Cuando el cifrado de 256 bits (*256-bit encryption*) está habilitado, el cliente TLS y el servidor TLS del SMC se configuran automáticamente para usar TLSv1.2 y suites de cifrado determinadas (ver apartado 6.4.1 CONFIGURACIÓN DE TLS).

6.2 AUTENTICACIÓN

6.2.1 SERVIDOR DE DIRECTORIO Y SERVIDOR DE AUTENTICACIÓN

59. El servidor de directorio (*Directory Server*) que contiene toda la información de usuarios y grupos, puede ser el Servidor de Gestión (LDAP interno), o un servidor externo.

60. Respecto al servidor de autenticación, hay que indicar que el proceso de autenticación utilizará la información de usuario, pero se implementa como una operación separada que no tiene por qué llevarse a cabo necesariamente en el mismo servidor que almacena la información de usuarios. El servidor de autenticación, por lo tanto, puede ser el Servidor de Gestión, o un servidor externo.

61. La siguiente tabla indica las combinaciones posibles respecto a los servidores de directorio y servidores de autenticación, y las características de estas combinaciones.

		Servidor de Autenticación (Proceso de autenticación)	
		Servidor de Gestión	**Servidor Externo**
Servidor de Directorio (información de usuarios y grupos)	**Servidor de Gestión**	• El Cliente de Gestión puede gestionar la información de usuarios y grupos. • La información de usuarios y grupos se puede usar para crear reglas. • Mecanismos de autenticación: contraseña, certificado o claves pre-compartidas (PSK). **No se recomienda el uso de claves pre-compartidas.**	• El Cliente de Gestión puede gestionar la información de usuarios y grupos. • No es posible permitir el acceso del servidor externo a la base de datos interna de información de usuarios del Servidor de Gestión. Se requiere una réplica de la Base de Datos de usuarios, en el servidor externo. • La información de usuarios y grupos se puede usar para crear reglas. • Mecanismos de autenticación: cualquiera implementado por el servidor externo.
	Servidor Externo	• El Servidor de Gestión se define como cliente LDAP para el servidor externo. La base de datos de usuarios no se replica en el Servidor de Gestión, sino que esta lanza una consulta al servidor externo cada vez que necesita esta información. • El cliente de gestión solo muestra las cuentas de usuario (lanzando consultas al servidor externo a través del Servidor de Gestión). • La información de usuario se puede usar para crear reglas. • Mecanismos de autenticación: contraseña, certificado o claves pre-compartidas (PSK). **No se recomienda el uso de claves pre-compartidas.**	• Opcionalmente, el servidor de Gestión se puede definir como cliente LDAP para el servidor externo. • Opcionalmente, se puede mantener de forma manual la misma información de usuario en el Servidor de Gestión, y en servidor externo. • En caso contrario, se puede crear un único elemento usuario "externo" para representar todos los usuarios que se almacenan en el servidor externo. En este caso, no es posible crear reglas diferentes para distintos usuarios externos. Cada regla de autenticación afectaría a todos los usuarios externos. • Mecanismos de autenticación: cualquiera implementado por el servidor externo.

Tabla 1 – Posibilidades de Servidores de Autenticación y Directorio

62. La opción más sencilla es utilizar el servidor LDAP interno del Servidor de Gestión cuando no existan necesidades específicas de usar un servidor LDAP externo. En este caso, la información de usuarios y grupos se almacena en el Servidor de Gestión. Cada cortafuegos almacenará una réplica de la base de datos de usuarios, de forma que cualquier cambio en la base de datos principal se replica inmediatamente en este. De esta forma, el cortafuegos puede acceder a sus directorios locales en lugar de comunicarse constantemente a través de la red con el Servidor de Gestión.

63. Para obtener más información sobre el uso y configuración de servidores de directorio y autenticación, tanto externos como locales, consultar el capítulo Setting up directory servers de la guía Forcepoint Next Generation Firewall Product Guide [REF1].

6.2.2 AUTENTICACIÓN DE USUARIOS

64. Los elementos Usuario (*User*) y Grupo de usuarios (*User Group*), definen la información de una cuenta de usuario para los usuarios finales. Al menos debe existir un elemento Grupo (Grupo de usuarios). Un usuario puede pertenecer a varios grupos.

65. A la hora de dar de alta un elemento Grupo, se configuran los métodos de autenticación (*Authentication Methods*) permitidos para los usuarios que formarán parte de él.

66. El elemento usuario define quién es el usuario y cómo se va a identificar a sí mismo para obtener el acceso a las redes y servicios según se defina en las reglas de acceso del cortafuegos. Se recomienda crear una cuenta de usuario individual para cada usuario. Cuando se da de alta un usuario, se seleccionará el método de autenticación de entre los permitidos en el Grupo.

67. Los posibles métodos de autenticación son los siguientes:

    a) **Basado en certificado, que es el método recomendado.**

    b) Basado en contraseña, siguiendo la política de establecimiento de contraseñas anteriormente indicada.

    c) Basado en claves pre-compartidas (*pre-shared keys*). Este método de autenticación no deberá usarse salvo que sea posible determinar a priori si la clave posee la fortaleza necesaria para garantizar el nivel de seguridad exigido por el sistema (ENS Categoría Alta exige una fortaleza de 128 bits).

    d) Cualquier método de autenticación implementado en servidores externos que soporten los protocolos RADIUS o TACACS+.

68. Para obtener más información la configuración de usuarios y grupos, y los métodos de autenticación, consultar el capítulo *Setting up user authentication* de la guía *Forcepoint Next Generation Firewall Product Guide* [REF1].

6.2.3 REGLAS DE ACCESO PARA AUTENTICACIÓN

69. Con conexiones VPN siempre es obligatoria algún tipo de autenticación. También se puede requerir autenticación para accesos que no van por VPN. Los parámetros de autenticación se definen en el campo *Authentication* de la regla:

Figura 3 – Ejemplo de campo *Authentication* en la regla del cortafuegos

70. Se activará un método de autenticación cuando, al menos, esté instalada en el cortafuegos una regla que contenga ese método de autenticación. La autenticación está asegurada durante un tiempo específico (*timeout* de autenticación) basado en la dirección IP origen.

71. Una vez que el usuario se autentica de forma satisfactoria, el cortafuegos añade el usuario a su lista de usuarios autenticados. La siguiente conexión que abra el usuario ya hará coincidencia (match) de forma automática con la regla de acceso que requiera autenticación si el usuario y el método de autenticación coinciden con los parámetros de la regla.

72. Para obtener más información sobre la configuración de Reglas de Acceso, consultar el tema *Define IPv4 Access rules for authentication* del capítulo *Setting up user authentication* de la guía *Forcepoint Next Generation Firewall Product* Guide [REF1].

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

73. **El sistema se deberá configurar de acuerdo con los principios de mínima funcionalidad y mínimo privilegio**, es decir, se tratará de que los usuarios administradores sean los mínimos posibles y que el conjunto de usuarios en general no disponga de más privilegios que los que necesita.

74. La administración del sistema se llevará a cabo a través del SMC, que ofrece dos (2) interfaces de administración:

    a) CLI (*Command Line Interface*) a través de consola, conectando un terminal directamente al puerto consola del dispositivo. La administración CLI tiene funcionalidades limitadas.

    b) GUI (*Graphic User Interface*) a través del Cliente de Gestión, que se conecta al Servidor de Gestión del SMC Appliance a través de TLSv1.2 y que permite todas las demás funciones de gestión no accesibles desde CLI. Para más información acerca de la configuración de comunicaciones seguras mediante el protocolo TLS, se recomienda consultar el apartado 6.4.1 CONFIGURACIÓN DE TLS, de este documento.

75. Como se ha comentado en apartados anteriores, cuando el sistema opera en un modo seguro, la consola local del *NGFW Engine* y el acceso SSH a este no están disponibles. Los *NGFW Engines* deberán configurarse desde el SMC a través del Cliente de Gestión.

76. El Cliente de Gestión será, por lo tanto, el que se utilice principalmente para configurar, controlar y monitorizar el sistema (SMC, *NGFW Engines*, e incluso monitorizar dispositivos de terceros).

6.3.1.1 CLIENTE DE GESTIÓN

77. Para establecer una conexión con el Cliente de Gestión al SMC (Security Management Center):

    a) Seleccionar *Add Server* e introducir la IP o nombre DNS del Servidor de Gestión.

    b) Introducir el nombre y contraseña del usuario administrador sin restricción de permisos (*superuser*) que se ha configurado durante la instalación del SMC.

    c) Pulsar *log on*.

78. El Cliente de Gestión dispone de varias vistas. Se utilizará la vista *Configuration view* para visualizar, cambiar y añadir información de configuración al sistema. Esta vista tiene varios módulos para poder configurar diversos elementos:

    a) *NGFW*, para gestionar los elementos NGFW Engine y configurar sus políticas.

    b) *Network Elements*, para gestionar varios hosts, redes y servidores.

    c) *VPN*, para configurar conexiones VPN, Servidores VPN y portales VPN SSL.

    d) *Administration*, para gestionar el sistema, incluyendo derechos de acceso, actualizaciones, licencias, cuentas de administración, alertas y escalado.

    e) *Monitoring*, para crear informes estadísticos, diagramas y configurar otras características relacionadas con la monitorización.

    f) *User Authentication*, para configurar las características de la autenticación de usuarios y servicios de directorio, y gestionar las cuentas de usuario.

79. A través de la vista de Global System Properties se podrán configurar parámetros globales del sistema:

    a) *Updates*, para configurar parámetros relativos a updates, upgrades y licencias.

    b) *Change Management*, para configurar la opción de forzar flujos de aprobación. Es posible establecer que los cambios que tengan efectos en la configuración actual tengan que ser aprobados antes de ser aplicados. Se puede permitir a los usuarios con rol de administrador que ellos mismos puedan aprobar sus propios cambios, tal y como se muestra en la imagen siguiente:

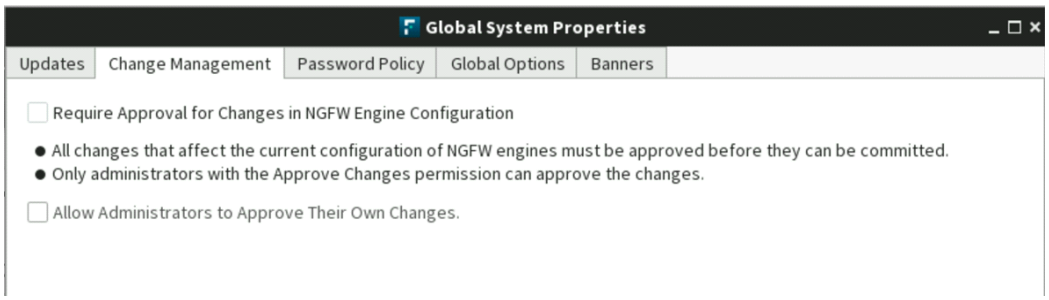

Figura 4 – *Change Management*

    c) *Password Policy*, para configurar los parámetros de la política de contraseñas.

    d) *McAfee Services*, para configurar el uso de *McAfee® Global Threat Intelligence™ y McAfee® Threat Intelligence Exchange*. Estos servicios ya vienen incluidos en el producto.

e) *Logon Banner*, para configurar el mensaje de inicio de sesión para administradores.

80. Para obtener más información sobre el cliente de gestión, consultar el capítulo *Using the Management Client* de la guía *Forcepoint Next Generation Firewall Product Guide* [REF1].

6.3.1.2 CUENTAS DE ADMINISTRACIÓN

81. Las cuentas de administración son las que permitirán a los administradores configurar y monitorizar el SMC y los NGFW Engines.

82. Como se ha comentado anteriormente, durante la instalación del *SMC Appliance* se crea automáticamente la cuenta de administración sin restricción de permisos (*superuser*), que se utilizará para crear las demás cuentas de administración.

83. Las cuentas de administración se dan de alta y se configuran en el SMC utilizando el Cliente de Gestión. Las cuentas y contraseñas de administración de consola local se gestionan, también, desde el SMC. Solo tienen acceso a consola local del SMC Appliance las cuentas de administración sin restricción de permisos (*superuser*).

84. Cada cuenta vendrá representada por un elemento Administrator que llevará asociados, a su vez, otros elementos para definir los permisos, derechos, mecanismos de autenticación, etc. Por lo tanto, antes de dar de alta el elemento Administrator, es necesario definir:

    a) Los permisos y derechos de acceso de la cuenta. Hay dos niveles de permisos para un administrador:

        - *Permisos sin restricción,* que permiten al administrador gestionar todos los elementos del sistema sin limitaciones, y ejecutar scripts que requieren de autenticación.
        - *Permisos restringidos*, que permiten definir en detalle qué permisos tendrá el administrador utilizando los elementos *Administrator role*, y sobre qué componentes del sistema, a través de los elementos *Access Control Lists*.

    b) El mecanismo de autenticación del administrador, que puede ser de dos (2) tipos:

        - *Autenticación local* mediante contraseña almacenada en la base de datos interna del SMC (Servidor de Gestión).
        - *Autenticación remota* con un servidor externo de autenticación a través de los protocolos RADIUS o TACACS+. Para más información al respecto, se recomienda consultar el apartado "*Authenticate administrators using RADIUS or TACACS+ methods*", de la Forcepoint Next Generation Firewall Product Guide [REF1].

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

85. Las acciones que podrá realizar el administrador se determinan a través de los elementos Administrator role. Hay 4 roles predefinidos, pero también se pueden crear roles a medida.

    a) *Viewer*, solo puede ver las propiedades de los elementos seleccionados.

    b) *Operator*, puede visualizar las propiedades de los elementos seleccionados y enviar comandos a los NGFW Engines, refrescar políticas, cargar políticas y buscar logs y alertas en los elementos seleccionados.

c) *Owner*, puede visualizar las propiedades, borrar o modificar los elementos seleccionados.

d) *Editor*, puede crear, editar y borrar los elementos seleccionados, y enviar comandos a los NGFW Engines, refrescar políticas, cargar políticas y buscar registros de eventos y alertas en los elementos seleccionados.

86. Para más información acerca de los roles de usuarios de administración, así como la configuración de los mismos, se recomienda consultar el Capítulo 21 "*Administrator accounts*", de la *Forcepoint Next Generation Firewall Product Guide* [REF1].

6.3.2.1 POLÍTICA DE CONTRASEÑAS Y PARÁMETROS DE SESIÓN

87. **Deberá definirse una política de contraseñas, que deberá estar en consonancia con la política de contraseñas de la organización, y aplicarla por defecto a todas las cuentas de administración.** Los parámetros a definir, serán los siguientes:

a) Número máximo de sesiones concurrentes.

b) Tiempo máximo de inactividad de sesión (*Idle timeout*). La sesión se bloqueará tras 5 minutos de inactividad.

c) Número máximo de intentos fallidos de autenticación (*Failed logon attempts*) y acciones a realizar cuando se supera el umbral. Este número no debería ser superior a 3 intentos.

d) Inhabilitación automática de cuentas inactivas.

e) Requisitos de vigencia, expiración y fortaleza de contraseñas. Deberán seguirse las siguientes directrices y opciones de configuración:

- No deberá permitirse la repetición de al menos las 5 últimas contraseñas utilizadas.
- No deberá realizarse un nuevo cambio de contraseña en los 10 días posteriores al último cambio.
- Deberán ser de 12 caracteres como mínimo, aunque se recomienda una longitud de 15 caracteres (parámetro *Minimum Amount of Mandatory Characters*).
- Deberán incluir caracteres alfanuméricos y caracteres especiales como "!", "@", "#", "$", "%", "^", "&", "*", "(" y ")", al menos una letra en mayúscula y otra en minúscula, un número o más, y un signo de puntuación o más.
- Deberán contener un número mínimo de juegos de caracteres o de cambios en el juego de caracteres.

f) Además, a la hora de seleccionar contraseñas para las cuentas de administrador autorizadas, conviene seguir las siguientes recomendaciones de seguridad:

- Deberán cambiarse periódicamente, con un período no superior a 60 días.

88. Para definir la política de contraseñas se debe hacer *login* con una cuenta de administración que tenga permisos de gestión sobre los elementos *Administrator*, o permisos sin restricciones. En caso de que se hayan configurado dominios, es necesario haber hecho login en el *Shared Domain*.

89. Para más información sobre el proceso a seguir para definir la política de contraseñas, se recomienda consultar el apartado "*Enable and define password policy settings",* de la *Forcepoint Next Generation Firewall Product Guide* [REF1].

6.3.2.2 CONFIGURACIÓN DEL LOGIN BANNER

90. El mensaje de inicio de sesión (*Login Banner*) es un mensaje que se muestra a los administradores, tanto en el acceso CLI de consola como en el acceso desde el Cliente de Gestión, antes de que realicen el *login*. **En el sistema no aparece por defecto ningún mensaje, por lo que deberá configurarse.**

91. Este mensaje deberá advertir que solo los usuarios autorizados pueden acceder al Sistema y que toda la actividad será supervisada para verificar el cumplimiento de la política de seguridad. Además, en dicho mensaje no se facilitará información del Sistema que pueda identificarlo o caracterizarlo ante un atacante.

92. Para configurar el mensaje, desde el Cliente de Gestión, con un usuario administrador sin restricción de permisos en el dominio compartido (*Shared Domain*), deberán seguirse los siguientes pasos:

    a) Seleccionar Menu > System Tools > Global System Properties.

    b) Hacer clic en *Logon Banner tab*.

    c) Seleccionar *Show Logon Banner* (ya que, por defecto, no se muestra ningún banner en el login).

    d) Escribir el texto que se desea mostrar en el banner.

93. Para más información al respecto, se recomienda consultar el apartado "*Create logon banners and export banners*", de la *Forcepoint Next Generation Firewall Product Guide* [REF1].

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

94. Cuando el sistema opera en el modo de operación seguro, protege las comunicaciones establecidas entre sus componentes o con otras entidades externas, de la siguiente forma:

    a) La conexión entre los Servidores del SMC Appliance (Servidor de Gestión y Servidor de Registro), se realiza a través del interfaz interno de *loopback*. Esta comunicación proporciona protección a la información de configuración intercambiada entre el Servidor de Gestión y el de Registro.

    b) La conexión entre el SMC Appliance y los NGFW Engines será una conexión directa establecida a través de una red dedicada. Esta comunicación proporciona protección a los registros de auditoría que el NGFW Engine envía al Servidor de Registro, y a la información de configuración intercambiada con el Servidor de Gestión.

    c) La conexión entre el Servidor de Registro y el Servidor de Gestión, y un servidor Syslog externo, se realiza a través del protocolo seguro TLSv1.2. Este protocolo proporciona protección a los registros de auditoría que ambos servidores envían al servidor Syslog externo.

    d) La conexión entre el Cliente de Gestión, y los Servidores de Gestión y de Registro, se realiza a través del protocolo seguro TLSv1.2. Este protocolo proporciona protección a

los registros de auditoría que el Cliente de Gestión envía al Servidor de Registro, y a la información de configuración intercambiada con el Servidor de Gestión.

6.4.1 CONFIGURACIÓN DE TLS

95. Las conexiones protegidas con protocolo TLS llevarán asociado un elemento TLS Profile. Estos elementos contienen la configuración de parámetros TLS: versión de protocolo, parámetros criptográficos y CA de confianza permitidas.

96. Los pasos para dar de alta un TLS profile son los siguientes:

    a) Desde *Configuration*, navegar a *Administration*.

    b) Seleccionar *Certificates > Other Elements > TLS Profiles.*

    c) Botón derecho en *TLS Profiles*, seleccionar *New TLS Profile*.

    d) Añadir el *Name*, para identificarlo posteriormente.

    e) Seleccionar la versión y las suites de cifra TLS.

    f) Seleccionar las CA de confianza permitidas:

        - Opción *Trust Any*, para permitir cualquier CA de las definidas como *Trusted Certificate Authorities*.
        - Opción *Trust Selected > Add*, para permitir solo un subconjunto de las *Trusted Certificate Authorities*.

    g) Configurar el resto de parámetros, OK.

97. Cuando el sistema opera en el modo de operación segura (FIPS mode y cifrado de 256 bits habilitado), el cliente y servidor TLS del SMC Appliance se configuran automáticamente con los siguientes parámetros:

    a) Versión de TLSv1.2.

    b) Suites de cifrado aceptadas por los Servidores de Gestión y de Registro:

        - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
        - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

        Donde:

        - Las curvas usadas en el algoritmo ECDHE para establecimiento de clave (Key Establishment) son: P-521, P-384, y P-256.
        - El algoritmo de firma es ECDSA P-521 / SHA-512.

98. Para obtener más información sobre la configuración de TLS, consultar el *tema Enabling TLS protection for traffic to external servers*, del capítulo *Configuring Systems Communications* de la guía *Forcepoint Next Generation Firewall Product Guide* [REF1].

6.5 GESTIÓN DE CERTIFICADOS

99. Para llevar a cabo la autenticación a través de certificado en las conexiones TLS, el Servidor de Registro y el Servidor de Gestión deben disponer de sus correspondientes certificados. Los certificados son necesarios para la autenticación de cliente en las conexiones con un

servidor externo de auditoría y para la autenticación de servidor en las conexiones con los Clientes de Gestión.

100. Para ello, el Servidor de Gestión dispone de dos CA internas (*Certificate Authority*) capaces de firmar certificados RSA o ECDSA. Sin embargo, se recomienda el uso de CAs externas. Para más información, se recomienda consultar el apartado "Type*s of internal certificate authorities*", de la guía *Forcepoint Next Generation Firewall Product Guide* [REF1].

101. La información acerca del proceso de creación de certificados, así como la gestión de CSRs (*Certificate Sign Requests*) se puede consultar en el apartado "*Creating certificates*", así como el apartado "*Create a certificate request*", de la guía *Forcepoint Next Generation Firewall Product Guide* [REF1].

102. Para obtener más información acerca del proceso a seguir para la gestión de certificados para la autenticación TLS, consultar el tema *Using certificates to secure communications to external components* del capítulo *Configuring System Communications* de la guía *Forcepoint Next Generation Firewall Product Guide* [REF1].

6.6 SERVIDORES DE AUTENTICACIÓN

103. Autenticación remota con un servidor externo de autenticación a través de los protocolos RADIUS o TACACS+. Para más información al respecto, se recomienda consultar el apartado *"Authenticate administrators using RADIUS or TACACS+ methods*", de la *Forcepoint Next Generation Firewall Product Guide* [REF1].

104. Asimismo, se recomienda consultar el apartado "*Create RADIUS or TACACS+ Authentication Server elements*", de la *Forcepoint Next Generation Firewall Product Guide* [REF1].

6.7 SINCRONIZACIÓN

105. **Se debe configurar el SMC Appliance para el uso de servidores NTP, de forma que todos los dispositivos puedan llevar a cabo el registro de eventos de forma precisa**. Esto se configurará a través del Cliente de Gestión.

106. Por defecto, SMC Appliance utiliza los servidores públicos NTP de Forcepoint. El Servidor de Gestión y el Servidor de Registro se sincronizan con la fecha/hora del SMC Appliance. Los NGFW Engines se sincronizan automáticamente con la fecha/hora del Servidor de Gestión. Esta opción se utilizará únicamente cuando no se disponga de un servidor NTP propio.

107. Los pasos para llevar a cabo la configuración NTP desde el Cliente de Gestión son los siguientes:

    a) Desde el Cliente de Gestión, seleccionar *Home > Others > Management Server*.

    b) Botón derecho en Management Server > Properties.

    c) Hacer click en *NTP tab*.

    d) Seleccionar Enable NTP server Synchronization.

    e) Para añadir un servidor NTP, pulsar *Add* y seleccionar el servidor NTP deseado.

108. En caso de ser necesario establecer la fecha/hora de forma manual en el SMC Appliance, ejecutar el siguiente comando:

    sudo date –s '<YYYY-MM-DD hh:mm:ss>'

109. A continuación, se enumeran los pasos a seguir para configurar el SMC Appliance para usar servidores NTP externos:

    a) En el Cliente de Gestión, seleccionar *Menu > System Tools > Global System Properties.*

    b) En la pestaña NTP, seleccionar *Enable time synchronization from NTP server.*

    c) Para añadir una fila a la tabla, hacer *click en Add.*

    d) Para añadir un servidor NTP, hacer click derecho en la casilla NTP Server, seleccionar Select, y a continuación seleccionar un elemento NTP Server.

    e) (Opcional) Si hay más de un servidor NTP, seleccionar el servidor NTP deseado.

    f) Hacer *click* en OK.

110. Para obtener más información, consultar el tema *Enable NTP time synchronization on the SMC Appliance* del capítulo *Configuring system communications* de la *guía Forcepoint Next Generation Firewall Product Guide* [REF1].

111. A continuación, se enumeran los pasos a seguir para habilitar la sincronización NTP para los NGFW Engines. Estos pueden ser configurados para emplear servidores NTP externos.

    a) Seleccionar *Configuration.*

    b) Hacer click derecho en un NGFW Engine, y a continuación seleccionar *Edit <element type>.*

    c) En el panel de navegación de la izquierda, ir a *General > NTP.*

    d) Seleccionar *Enable time synchronization from NTP server.*

    e) Para añadir una fila a la tabla, hacer *click* en *Add*.

    f) Para añadir un servidor NTP, hacer *click* derecho en la casilla NTP Server, seleccionar *Select*, y a continuación seleccionar un servidor NTP.

    g) (Opcional) si hay más de un servidor NTP disponible, seleccionar el servidor NTP deseado.

    h) Hacer click en *Save and Refresh*.

112. Si un NGFW Engine es configurado para utilizar sincronización NTP, y puede conectarse con éxito a un servidor NTP externo, el NGFW Engine ignora los comandos de configuración de tiempo del Servidor de Administración.

113. Para más información al respecto, se recomienda consultar el apartado "*Enable NTP time synchronization for NGFW Engines*", de la guía *Forcepoint Next Generation Firewall Product* Guide [REF1].

6.8 ACTUALIZACIONES

114. Las actualizaciones y parches del SMC Appliance y de los NGFW Engines, deben ser aplicados siguiendo las directrices indicadas en el capítulo *Maintenance and upgrades* de la guía *Forcepoint Next Generation Firewall Product Guide* [REF1], para garantizar que la actualización sea segura.

115. La versión del Cliente de Gestión debe ser la misma que la versión del SMC Appliance.

116. Las actualizaciones de SMC Appliance y NGFW Engine, se verifican utilizando mecanismos criptográficos (ECDSA P-521 con firmas digitales SHA-512 y una clave pública preinstalada).

117. Los comandos utilizados para actualizar SMC Appliance verifican la firma digital y rechazan cualquier actualización que no sea válida.

118. En actualizaciones del NGFW Engine, SMC verifica la firma de la actualización del NGFW Engine cuando se importa la actualización al SMC. Solo se pueden importar e instalar las actualizaciones válidas en el NGFW Engine.

119. El proceso de actualización es el siguiente:

    a) Descargar el fichero del parche del SMC Appliance desde la URL de Forcepoint y guardarlo en un USB.

    b) Conectar la unidad USB al SMC Appliance y montarla a través del comando:

        $ sudo mount /dev/sdb1 /mn

    c) Cargar el parche a través del siguiente comando:

        $ sudo ambr-load –f /mnt/6.10.1P001.sap

    d) Instalar el parche a través del siguiente comando:

        $ sudo ambr-install 6.10.1P001

120. Cuando se instala el parche, el sistema crea automáticamente una copia de respaldo de la configuración y un *snapshot* del sistema de ficheros antes de efectuar la instalación.

121. Después de una actualización, se puede regresar el *SMC appliance* a la versión previa, si es necesario (roll back). Sin embargo, todos los cambios que se hayan producido en la configuración tras la actualización se perderán. El roll back se puede hacer desde línea de comandos*: #sudo smca-system toggle.*

6.9 AUTO-CHEQUEOS

122. Cuando el SMC Appliance se inicia, se ejecutan automáticamente una serie de auto-tests (*self-tests*): KAT (*Known answer tests*) y PCT (*Pairwise consistency Test*), sobre los algoritmos y funciones criptográficas y sobre la integridad del software.

123. Debe revisarse en la consola el resultado de la ejecución de estos auto-test. Si han sido correctos, se continuará con la configuración del SMC Appliance. Si no lo han sido y el SMC Appliance no se reinicia de forma automática, se debe reiniciar de forma manual. En caso de que tras el reinicio manual continúe fallando el resultado de la ejecución de los tests siga siendo negativo, será necesario resetear el SMC Appliance a los parámetros de fábrica.

124. NGFW Engine contiene *OpenSSL FIPS Object Module, NGFW Cryptographic Library*, y NGFW *Cryptographic Kernel Module*. Estos módulos ejecutan los siguientes *auto-tests (self-tests*) cuando arranca el *appliance*:

    a) *Cryptographic algorithm known answer tests (KAT).*

    b) Test de integridad del software usando la función HMAC.

    c) *Auto-tests condicionales* para la función CTR-DRBG.

    d) *Pair-wise consistency test* (PCT) sobre las claves RSA, DSA y ECDSA generadas.

    e) Chequeo de la integridad de *File Systems,* usando el *OpenSSL FIPS Object Module* y la función HMAC.

6.10 AUDITORÍA

6.10.1 REGISTRO DE EVENTOS

125. El sistema permite visualizar logs, alertas y registros de auditoría a través de las vistas del panel de log (*Logs View*). Se pueden ver datos de los servidores SMC, de los NGFW Engines y de componentes de terceras partes que hayan sido configurados para enviar datos al SMC. Se pueden ver y analizar, por lo tanto, muchos tipos de datos procedentes de muchos tipos de componentes, de forma individual o conjunta.

126. Para obtener más información sobre la visualización de logs, consultar el capítulo *Viewing and exporting logged data* de la guía *Forcepoint Next Generation Firewall Product Guide* [REF1]

127. Los contenidos de los registros de eventos y auditoría se muestran en el formato McAfee ESM. En la siguiente tabla se describen algunos de los campos más comunes de este formato:

EVENTO	EJEMPLO DE REGISTRO GENERADO
Timestamp	Hora de creación de entrada en el registro
Node ID	Dirección IP del motor o servidor que envió la entrada del registro.
Facility	Subsistema de cortafuegos que creó la entrada de registro.
CompId	Identificador del creador de la entrada del registro.
InfoMsg	Descripción del evento de registro que explica más la entrada.
SenderType	Tipo de motor o servidor que envió la entrada del registro.
EventId	Identificador de evento, único dentro de un emisor.
UserOriginator	Administrador que activó el evento de auditoría.
ClientIpAddress	Dirección del cliente que activó el evento de auditoría.
Type	Tipo de gravedad de entrada de registro.
TypeDescription	Tipo de acción que activó la entrada de auditoría.
Result	Estado del resultado tras el evento auditado.
ObjectName	Elementos que se van a manipular en el evento de auditoría.
SituationId	Identificador de la situación que activó el evento de registro.
Situation	Nombre de situación.

Tabla 2 – Campos del formato de registro de eventos y auditoría

6.10.2 ALMACENAMIENTO LOCAL

128. El mayor consumidor de almacenamiento es el proceso de registro. Los datos de registro se envían en tiempo real al Servidor de Registro en condiciones normales, por lo que no se consume una gran cantidad de espacio en disco en el firewall. En caso de fallo en las

comunicaciones entre *Next Generation Firewall* y el Servidor de Registro, los registros se guardan en la unidad local hasta que se restablecen las comunicaciones y después se transfieren gradualmente al Servidor de Registro.

129. Los registros de auditoría contienen información acerca de las acciones realizadas en el sistema y los eventos generados en el sistema.

130. En caso de que el Servidor de Registro tenga su espacio de almacenamiento cercano al límite, el comportamiento es el siguiente:

    a) Cuando el espacio libre de almacenamiento para auditoría cae por debajo de los 300 MB, se envía una alerta a los administradores que se muestra en el Cliente de Gestión.

    b) Cuando quedan menos de 100 MB de espacio, el Servidor de Registro deja de aceptar nuevos mensajes de auditoría de los NGFW Engines. El administrador tiene que eliminar registros de auditoría antiguos de forma manual.

131. El NGFW Engine almacena localmente el registro generado y se lo envía al Servidor de Registro. Solo cuando este confirme la recepción del registro, el NGFW Engine lo borra de su almacenamiento local. En caso de que el NGFW Engine no pueda enviar sus registros al Servidor de Registro, continuará almacenándolos localmente hasta que se solucione el problema y pueda enviarlos, empezando por los más antiguos y borrándolos cuando todos ellos hayan sido enviados.

132. En caso de que el NGFW Engine no pueda transferir los registros durante un tiempo prolongado, existe la posibilidad de que agote su espacio de almacenamiento local (el espacio disponible depende del modelo). En caso de que esto ocurra, el administrador debe definir qué acción se va a realizar. La acción recomendada es la de Stop Traffic, que evita la pérdida de posibles registros al pasar el NGFW Engine automáticamente a estado offline, transfiriendo las conexiones que estaba gestionando a otro nodo del cluster (en caso de que forme parte de uno). Esta acción de Stop Traffic se define en el parámetro *Log Spooling Policy*, dentro de *Engine Editor > Advanced Settings > Log handling*.

133. El examen de los registros de auditoría permite, por ejemplo, realizar un seguimiento de qué tipo de acciones de administrador se han realizado y quién las ha realizado. Estos datos pueden ser importantes a la hora de identificar posibles errores de configuración y otros eventos comparables.

134. Los registros de auditoría pueden examinarse en el explorador de registros (Log Browser). Puede especificar qué tipos de acciones le interesan y en qué periodo de tiempo. Esto permite realizar un seguimiento preciso de todos los eventos del sistema o acciones de administrador, y ayuda a mantener la integridad del sistema.

135. Para obtener más información sobre los registros de auditoria consultar el capítulo "*Log data management and how it Works*" de la guía *Forcepoint Next Generation Firewall Product Guide* [REF1].

6.10.3 ALMACENAMIENTO REMOTO

136. Es recomendable enviar los registros de auditoría almacenados en el Servidor de Gestión y en el Servidor de Registro a un servidor externo de auditoría. Esto, además de solucionar el problema del espacio limitado de almacenamiento local, permite que los datos sean procesados en un sistema externo. Es posible definir qué tipo de datos de auditoría se quieren reenviar y en qué formato.

137. Este tráfico de registros de auditoría debe ir protegido a través de TLS, por lo que, antes de proceder a la configuración de las reglas para el reenvío de logs y registros, deberán seguirse los siguientes pasos:

    c) La CA emisora del certificado del servidor externo de auditoría, debe formar parte de las CAs de confianza del SMC Appliance (*Trusted Certificate Authorities*), para lo cual, se deberá haber importado previamente su certificado raíz (*CA root certificate*).

    d) El Servidor de Gestión y el Servidor de Registro, deben disponer de sus propios certificados para la autenticación de cliente TLS de la conexión. Estos certificados pueden haber sido emitidos por una CA interna (*Internal Certificate*) o por una CA externa (*Imported Certificate*). Se recomienda esta última opción, para lo cual, la CA emisora de este certificado, también debe formar parte de las CAs de confianza (*Trusted Certificate Authorities*).

    e) Deberá haberse configurado un *TLS profile* con los parámetros de la conexión TLS. Ver apartado 6.4.1 CONFIGURACIÓN DE TLS.

    f) Deberá haberse habilitado en la correspondiente política, el registro (*logging*) del tráfico que se desea monitorizar. Para ello, se debe editar la regla de la política que permite el tráfico a monitorizar, hacer doble clic en la celda *Logging*, y seleccionar las opciones de logging deseadas. Se puede consultar más información al respecto en el apartado *Enable logging for monitored traffic* del capítulo *Configuring the Log Server* de la guía *Forcepoint Next Generation Firewall Product Guide* [REF1].

138. Una vez completados los pasos del apartado anterior, para configurar el reenvío de logs a un servidor externo deberán seguirse los siguientes pasos:

    a) Desde el cliente de gestión, seleccionar *Home* y navegar *a Others > Log Server y Others > Management Server*.

    b) Botón derecho en el *Log Server / Management Server* desde el que se quiere reenviar los datos de log, seleccionar *Properties*.

    c) Pulsar en *Log Forwarding tab / Audit Forwarding tab.*

    d) Crear una nueva regla, pulsando *Add*.

    e) En *Target Host*, seleccionar el servidor externo al que se van a reenviar los datos de log.

    f) En *Service*, seleccionar ***TCP with TLS***.

    g) En los campos *Port, Format, Data Type* (solo para el Servidor de Registro), y *Filter*, seleccionar los parámetros según la configuración.

    h) En *TLS Profile*, seleccionar el *TLS Profile* que se habrá creado previamente con los parámetros adecuados para esta conexión TLS.

    i) Se recomienda utilizar *TLS server identity*, para determinar cómo se va a verificar la identidad del servidor Syslog al que se van a enviar los datos. Para ello:

        - *Doble-click* en TSL *Server Identity.*
        - Seleccionar el *identity type* que se va a usar para la verificación (normalmente, el *DNS name*). Se recomienda seleccionar "*Fetch from Certificate*", para obtener el dato de identidad, del certificado que presente el servidor Syslog.
        - En el campo de *identity value*, introducir el valor del campo de identidad esperado.

j) Seleccionar *Use Imported Certificate* y seleccionar el elemento *TLS credentials* que contiene los certificados previamente importados en el Servidor de Gestión y Servidor de Registro.

139. Para obtener más información, consultar el tema *Forwarding log data from Log Servers to external hosts*, así como el tema *Enable TLS protection for log or audit data forwarding* del capítulo *Configuring the Log Server* de la guía *Forcepoint Next Generation Firewall Product Guide* [REF1].

6.11 *BACKUP*

140. Las copias de seguridad permiten guardar y restaurar la configuración del Servidor de Registros y del Servidor de Gestión de Forcepoint en el mismo sistema o en otro host físico.

141. La copia de seguridad del Servidor de Gestión contiene políticas, elementos y otros detalles de configuración esenciales para todos los componentes que gestiona, así como la configuración del propio Servidor de Gestión.

142. La copia de seguridad del Servidor de Registro contiene la configuración local del servidor y, opcionalmente, los registros. La restauración de las copias de seguridad permite restaurar la configuración del Servidor de Gestión al mismo estado que cuando se realizó la copia de seguridad, aunque se restaure en una instalación completamente nueva.

143. Las copias de seguridad permiten recuperar la configuración del sistema; por ejemplo, en caso de un fallo del *hardware*. Una copia de seguridad permite reasignar los servidores de SMC a otro *hardware*.

144. Las copias de seguridad del Servidor de Gestión incluyen toda la información de configuración, incluidas las licencias, los certificados de los componentes del servidor necesarios para las comunicaciones del sistema, la CA raíz y las cuentas de usuario almacenadas localmente. La configuración creada en SMC para los componentes del motor se incluye en la copia de seguridad del Servidor de Gestión, por lo que no es necesario realizar copias de seguridad distintas para estos componentes.

145. Las copias de seguridad del Servidor de Registro contienen la información de configuración del Servidor de Registro. Se puede configurar el límite de tamaño de la copia de seguridad del Servidor de Registros.

146. Las copias de seguridad de Forcepoint Management Center creadas en un Sistema Operativo pueden restaurarse en una instalación con otro Sistema Operativo sin necesidad de tomar medidas especiales. Esto resulta práctico al cambiar el Sistema Operativo o la plataforma de hardware.

147. Cada vez que se realiza una copia de seguridad, se denomina el archivo con la fecha y hora para el control de versiones. El administrador también puede añadir comentarios y es recomendable cifrar el archivo con una contraseña. El archivo de copia de seguridad es un solo archivo zip. Por consiguiente, la gestión del archivo puede realizarse directamente en el sistema. Es a su vez recomendable activar tareas automáticas de backup.

148. Las claves privadas de los certificados de los NGFW Engine se almacenan localmente en los Engines y no se incluyen en las copias.

149. Las copias de seguridad deben realizarse siempre a través de la herramienta interna del Servidor de Gestión, no a través de herramientas externas.

150. Para obtener más información sobre los *backups*, consultar el capítulo "*Manteinance and upgrades*" de la guía *Forcepoint Next Generation Firewall Product Guide* [REF1].

6.12 FUNCIONES DE SEGURIDAD

6.12.1 VPN

151. El sistema permite crear dos tipos de VPN: basadas en políticas (*Policy-Based*) y basadas en rutas (*Rute-Based*).

152. En las VPN basadas en políticas, las reglas de acceso del cortafuegos determinan qué tráfico es enviado a través del túnel VPN. Estas VPN, a su vez, se dividen en:

    a) VPN de acceso remoto: conexiones a la red interna desde clientes remotos conectados desde redes externas (*mobile VPNs*). En estos tipos de VPN, se pueden usar túneles IPsec o SSL. Cada tipo de túnel se puede usar de manera independiente o de forma conjunta en una misma VPN basada en política.

    b) *VPN site-to-site*: conexiones entre servidores o *gateways* VPN, en las que alguno de los gateway VPN actúa como *gateway* central y otros actúan como *gateway* VPN satélites (por ejemplo, en topología estrella o *hub*).

153. En las VPN basadas en rutas, todo el tráfico encaminado hacia un interfaz del cortafuegos, configurado como extremo VPN, se envía a través de un túnel VPN. En este caso, solo es posible crear VPN *site-to-site* entre servidores o *gateways* VPN.

154. No es posible utilizar el mismo túnel VPN para varias configuraciones dentro de un mismo NGFW Engine.

155. Dependiendo de la complejidad de la configuración, pueden ser necesarias varias etapas para configurar una VPN (p. ej.: configuración de elementos *Gateway VPN, VPN Profile,* Certificados, reglas de acceso, etc).

156. Para obtener información detallada sobre cómo llevar a cabo la configuración de la VPN y todos sus elementos, consultar el capítulo *Configuring VPNs* de la guía *Forcepoint Next Generation Firewall Product Guide* [REF1].

157. Las negociaciones y el tráfico VPN se registran en los registros de auditoría como mensajes informativos, y pueden ser visualizados en la vista de Logs (*Logs View*) como cualquier otro tipo de log.

158. Las nuevas conexiones que sean aceptadas por una VPN basada en política, se registran en los logs igual que cualquier otro tráfico, en función de las opciones de registro configuradas en las reglas de acceso.

159. Si se producen problemas en relación con las conexiones VPN, es posible activar los diagnósticos IPsec en el cortafuegos para obtener más información.

6.12.2 VPN: AUTENTICACIÓN POR CERTIFICADOS

160. Para la autenticación de cada extremo en el establecimiento de una VPN, es posible usar los siguientes métodos de autenticación:

    c) Claves pre-compartidas (PSK**)**, lo que requiere que ambos extremos de la comunicación dispongan de la misma clave secreta. Este tipo de autenticación únicamente sería

adecuado cuando sea posible demostrar que la clave tiene la suficiente longitud y entropía, se mantiene en secreto y se renueva periódicamente. **En el resto de los casos, no se recomienda el uso de claves pre-compartidas.**

d) Certificados. En el caso de VPN site-to-site, ambos gateways VPN deben tener un certificado válido firmado por una CA reconocida por ambos. En el caso de VPNs de acceso remoto, al menos el servidor VPN debe tener un certificado válido, aunque se recomienda que el cliente también se autentique a través de un certificado.

161. Como se ha indicado anteriormente, **los certificados son el método de autenticación recomendado.** El Servidor de Gestión dispone de dos CAs internas para firma de certificados tipo RSA o ECDSA (*Internal RSA CA for Gateways, Internal ECDSA CA for Gateways*). Estos certificados son, por lo tanto, "auto-firmados" (*self-signed*), estas CAs no soportan CRL (*Certificate Revocation* List) y por lo tanto no se recomienda su uso.

162. **Se recomienda, por lo tanto, emplear CA externas**. Para ello, el sistema permite crear una petición CSR (*Certificate Signing Request*), enviarla a firma de la CA externa, e importarla en el *gateway* o en el cliente VPN.

163. El servidor o *gateway* VPN aceptará, por defecto, todos los certificados firmados por las CA que tenga dadas de alta el cortafuegos. Por ello, se deberá restringir la lista de CA aceptadas para las conexiones VPN. Esto se puede configurar en los parámetros del cortafuegos VPN *> Certificates.*

164. La configuración de los certificados firmados por CAs externas implica los siguientes pasos generales:

a) Importar el certificado raíz de la CA (*root CA certificate*), para declararla como confiable.

- *Configuration > VPN > Other Elements > Certificates > VPN Certificate Authorities.*
- Botón derecho en *VPN Certificate Authorities > New VPN Certificate Authority.*
- Click en import / Copy para importar o copiar el certificado.

b) Activar la comprobación de estado de los certificados. Los cortafuegos deberán comprobar el estado de revocación de los certificados firmados por esa CA, bien a través de listas CRL, o a través del protocolo OCSP. Es necesario tener en cuenta que los certificados serán tratados como inválidos hasta que no sean chequeados positivamente. Para configurar esta opción:

- En *Validation tab* seleccionar *Check Validity on Certificate-Specified CRLs*. Se pueden seleccionar más servidores CRL adicionales a los definidos en el certificado (*Add*).
- En *Validation tab* seleccionar *Check Validity on Certificate-Specified OCSP Servers*. Se pueden seleccionar más servidores OCSP adicionales a los definidos en el certificado (*Add*).

c) Limitar a un conjunto más reducido de CA cuando se realice la configuración de los elementos *VPN Gateway* y *VPN Profile*, dado que todas las CA configuradas serán consideradas de confianza por todos los gateways para todas las VPN.

d) Importar el certificado firmado por la CA externa. También es posible generar la petición CSR en el *gateway*, exportarla a la CA externa para firma, e importar el certificado firmado. Para generar la petición CSR:

- *Configuration > VPN > Gateways.*
- Botón derecho en el Gateway VPN > Tools > Generate Certificate. **Deberán seleccionarse certificados tipo RSA con tamaño de clave de 3072 bits o superior, o certificados ECDSA con curvas P-256 o superior.**

e) Una vez importados los certificados, para utilizarlos como método de autenticación, en el VPN profile seleccionar *certificate-based Authentication Method* en *IKE SA* tab.

6.12.3 VPN: CONFIGURACIÓN IPSEC

165. A la hora de configurar el elemento *VPN Profile* (que contiene los parámetros de autenticación, comprobaciones de integridad y cifrado IKE/IPsec), se definen los parámetros IKE / IPsec que utilizarán todas las VPNs que utilicen ese *VPN Profile*. Estos parámetros deben ser compatibles con los soportados por el servidor o *gateway* VPN extremo.

166. Dentro de los parámetros del *VPN Profile* habrá que configurar:

a) IKE SA tab. **Es necesario tener en cuenta lo siguiente:**

- Versión IKE. **Deberá utilizarse IKEv2.**
- Algoritmos de cifrado. Deberá utilizarse **AES con longitud de clave de, al menos, 128 bits.**
- Funciones Hash. Se recomienda el **uso de SHA-2 o superior** (*Minimum Length 256 bits).*
- **Grupos Diffie-Hellman. Deberán utilizarse los grupos: 15, 16, 19, 20, 21, 28, 29 o 30.**
- Método de autenticación. **Se recomienda el uso de certificado** (*certificate-based Authentication Method*).

b) IPsec SA tab. Dentro de los parámetros a configurar, **se debe tener en cuenta lo siguiente:**

- Tipo IPsec. **Deberá seleccionarse ESP.**
- Algoritmos de cifrado. Se recomienda el uso de **AES con longitud de clave de, al menos, 128 bits.**
- Funciones Hash. Deberá utilizarse **SHA-2 o superior** (*Minimum Length* 256 bits).
- Algoritmo de compresión. Se recomienda seleccionar None. En caso de que servidor VPN extremo lo soporte, deberá seleccionarse **Use PFS (*Perfect Forward Secrecy) with Diffie-Hellman Group*, con los Grupos *Diffie-Hellman*: 15, 16, 19, 20, 21, 28, 29 o 30.**

167. En caso de seleccionar otras opciones ofrecidas por el dispositivo para los algoritmos y funciones criptográficas, debe tenerse en cuenta que aquellas que se seleccionen deberán proporcionar siempre la fortaleza necesaria para garantizar el nivel de seguridad exigido por el sistema. **Para la cualificación de productos en Categoría ALTA del ENS exige una fortaleza de 128 bits. Se recomienda consultar la *guía CCN-STIC-807 Criptología de Empleo en el ENS* para más información.**

168. Para más información al respecto, se recomienda consultar el apartado "*Example VPN configuration 2: create a VPN Profile element", de la Forcepoint Next Generation Firewall Product Guide* [REF1].

6.12.4 POLÍTICAS DEL CORTAFUEGOS

169. Los NGFW Engines admiten o rechazan el tráfico según las reglas de filtrado del cortafuegos contenidas en una política de cortafuegos. **Un principio clave cuando se define la política del cortafuegos es seguir una aproximación basada en denegación por defecto (lógica positiva), que implica que selectivamente se permite únicamente lo estrictamente necesario.** Es decir, se habilita el tráfico permitido y el cortafuegos bloqueará todo lo demás a través de las reglas de rechazo y denegación total. Por el contrario, la aproximación de denegación selectiva (lógica negativa) se fundamenta en denegar todo aquello que no está permitido, lo cual es una práctica poco recomendable por su difícil gestión y porque deja una superficie de ataque mucho mayor.

170. Cada política, a su vez, se basa en una plantilla de política. Una plantilla de política contiene reglas predefinidas y también permite la creación de nuevas reglas.

171. Las reglas de acceso son reglas de gestión de tráfico que definen cómo se examina el tráfico, y qué acción realiza el NGFW Engine cuando se cumple una regla (match). Se pueden usar los valores de Origen, Destino y Servicio para establecer los criterios de filtrado de la regla.

172. Para obtener información adicional, se recomienda consultar *Configuring Access rules* del capítulo *Access rules* de la guía *Forcepoint Next Generation Firewall Product Guide* [REF1].

173. En conexiones con control de estado (*stateful connections*), solo se crea una entrada de registro (*log entry*) para el primer paquete que se detecta en la conexión de control o en la conexión de datos.

174. El tráfico TCP del puerto 21 se interpreta de forma predeterminada como el tráfico del protocolo FTP (RFC 959) gracias al Agente de protocolo FTP. Si las reglas de acceso permiten esta conexión de control y el tráfico del puerto 21 contiene comandos válidos del protocolo FTP para abrir una conexión de datos, el NGFW permite las conexiones de datos asociadas a dicha sesión de control y las registra utilizando los mismos criterios. Este tipo de sesiones se llaman sesiones dinámicas, ya que constan de una conexión de control y una de datos que se negocia en la conexión de control previa.

175. Para obtener más información sobre el Agente de protocolo FTP, consultar el *tema Define FTP Protocol parameters* del capítulo *Working with Service elements* de la guía *Forcepoint Next Generation Firewall Product Guide* [REF1].

176. Para obtener más información sobre las capacidades de establecimiento de sesiones dinámicas (sesiones en las que hay una conexión de control y una de datos), consultar el tema *How Multi-Layer inspection works* del capítulo *Introduction to Forcepoint NGFW* in *the Firewall/VPN role* de la guía *Forcepoint Next Generation Firewall Product Guide* [REF1].

6.12.5 CREACIÓN DE UNA PLANTILLA DE POLÍTICA DEL CORTAFUEGOS

177. Se recomienda añadir reglas de acceso específicas a una plantilla de política de cortafuegos personalizada y utilizar dicha plantilla para crear políticas de seguridad.

178. Las comprobaciones de validez de paquetes permiten descartar de forma automática paquetes IP no válidos, paquetes con ciertas opciones IP, paquetes IP incompletos y

fragmentos IP no válidos. Estos paquetes descartados también son registrados (*logged*) en caso de que estén habilitados los diagnósticos de filtro de paquetes.

179. La función de *anti-spoofing* automática elimina y registra (log) los paquetes falsificados (*spoofed*) en los que: la dirección origen o destino es una dirección de *loopback*, la dirección origen es una dirección de *broadcast* IPv4 o una dirección *multicast* IPv4, o la dirección origen no pertenece a una red conectada.

180. Las reglas de acceso adicionales en la plantilla personalizada, permiten descartar direcciones de enlace local IPv4 e IPv6, direcciones reservadas IPv6, direcciones reservadas IPv4 e IPv6 para uso futuro, y paquetes en los que la dirección origen sea una dirección multicast IPv6.

181. En el capítulo *Creating and managing policy elements* de la guía *Forcepoint Next Generation Firewall Product Guide* [REF1] se indican los pasos generales para crear una plantilla de política.

6.12.6 CREAR UNA POLÍTICA DE CORTAFUEGOS

182. Después de crear la plantilla de política de cortafuegos personalizada, se creará una política de cortafuegos basándose en esa plantilla.

183. Para obtener información adicional, consultar el tema *Considerations for designing Access rules* del capítulo *Access rules* y el capítulo *Creating and managing policy elements* de la guía *Forcepoint Next Generation Firewall Product Guide* [REF1].

184. Las reglas de acceso afectan a todas las interfaces de red, a menos que se especifique la interfaz de origen. Para obtener más información a este respecto, consultar el *tema Using Zone elements for interface matching in firewall Access rules* del capítulo *Access rules* de la guía Forcepoint Next Generation Firewall Product Guide [REF1].

185. Para configurar el registro (logging) de una regla, hacer doble clic en la celda *Logging* y configurar los ajustes. (ver apartado *Enable logging for Monitored traffic* del capítulo *Configuring the log server* de la guía *Forcepoint Next Generation Firewall Product Guide* [REF1]).

186. Los paquetes rechazados automáticamente, por defecto no se registran (*logged*). Para habilitar el *logging* de todos los paquetes, hacer clic con el botón derecho en el NGFW Engine, y seleccionar *Options > Diagnostics y en Packet Processing*, seleccionar *Packet Filtering.*

7. FASE DE OPERACIÓN

187. Para garantizar una gestión eficiente y segura del sistema, deberán llevarse a cabo, al menos, las siguientes tareas durante la fase de operación y mantenimiento:

a) **Comprobaciones periódicas del hardware y software** para asegurar que no se ha introducido hardware o software no autorizado. El código fuente del código activo y su integridad deberá verificarse periódicamente y estará libre de software malicioso.

b) **Programar la realización de copias de seguridad** automáticas de la configuración esencial almacenada en el Servidor de Gestión.

c) **Revisar la configuración de las actualizaciones automáticas** y asegurar que estas funcionan adecuadamente, de forma que se mantenga el sistema actualizado y con sus parches de seguridad aplicados.

d) **Configurar tareas automáticas para gestionar los datos de auditoría** y evitar que el espacio de almacenamiento del Servidor de Registro o del Servidor de Gestión llegue a su límite, afectando al comportamiento del sistema.

e) **Definir alertas y las correspondientes políticas de escalado** para mantener informados a los administradores, sobre los eventos críticos que ocurran en el sistema.

f) **Comprobación de que los registros de auditoría están protegidos** del borrado y modificación no autorizada, incluso accidentales.

g) **Control de acceso a la información de auditoría**, de forma que únicamente el personal de seguridad designado pueda acceder a ella.

h) Almacenamiento de la información de auditoria en las **condiciones establecidas en la normativa de seguridad y por el período establecido.**

8. REFERENCIAS

REF1 *Forcepoint Next Generation Firewall Product Guide*
https://www.websense.com/content/support/library/ngfw/v610/mgmt/ngfw_6100_pg_c_en-us.pdf

REF2 *Forcepoint Next Generation Firewall Installation Guide, version 6.10, revision A*
https://www.websense.com/content/support/library/ngfw/v610/install/ngfw_6100_ig_b_en-us.pdf

REF3 *How to install Forcepoint NGFW in FIPS mode, version 6.10, revision*
https://www.websense.com/content/support/library/ngfw/v610/install/ngfw_6100_ht_install-ngfw-in-fips-mode_b_en-us.pdf

REF4 *Forcepoint Next Generation Firewall Common Criteria Evaluated Configuration Guide*
https://www.niap-ccevs.org/MMO/Product/st_vid11234-agd.pdf

REF5 *Java Web Start*
https://www.java.com/es/download/help/java_webstart_es.html

9. ABREVIATURAS

CA Autoridad de Certificación (*Certification Authority*)

CC *Common Criteria*

CLI Interfaz de línea de comandos (*Command Line Interface*)

CRL Lista de revocación de certificados (*Certificate Revocation List*)

CSR Petición de certificado (*Certificate Signing Request*)

ENS Esquema Nacional de Seguridad.

FIPS *Federal Information Processing Standard*

GUI Interfaz gráfica (*Graphic User Interface*)

NGFW *Next Generation Firewall*

NTP *Network Time Protocol*

OCSP Protocolo de revisión de certificados online (*Online Certificate Status Protocol*)

PSK Claves pre-compartidas (*Pre-Shared Keys*)

SMC *Security Management Center*

SSH *Secure Shell*

SSL *Secure Socket Layer*

TLS *Transport Layer Security*

VPN *Virtual Private Network*

PUBLICACIONES DE DEFENSA

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