centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1469

Procedimiento de Empleo Seguro
Sophos Firewall SFOS v20.0

Mayo 2025

MINISTERIO DE DEFENSA

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

Edita:

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-25-202-3
Fecha de Edición: mayo de 2025

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2026.01.16 07:51:42 +01'00'

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. Sophos Firewall es un cortafuegos de red basado en software, que ofrece una solución integral de seguridad de red, a través de capacidades avanzadas de firewall. Las interfaces, a través de las cuales se pueden gestionar las funcionalidades que ofrece el producto, son las siguientes:
    a) CLI. Permite tanto acceso local (cable) como remoto mediante el protocolo SSH.
    b) Interfaz web. Accesible remotamente a través del protocolo HTTPS.
2. El firewall admite alta disponibilidad y rendimiento mediante la agrupación en clústeres y equilibrio de carga. Además, Sophos Firewall protege de accesos no autorizados mediante la creación de reglas, salvaguardando la red *LAN* en cuestión y la *DMZ* donde se encuentran los servidores delicados de la organización que instale el cortafuegos.
3. Alguna de las funcionalidades que Sophos Firewall proporciona, son las siguientes:
    a) Gestión de reglas y políticas de seguridad, incluidos los atributos de seguridad asociados.
    b) Configurar la protección de autenticación de usuarios y la autorización de estos, para realizar la configuración y creación de reglas.
    c) Registrar, buscar y filtrar logs de los eventos ocurridos en el comienzo, transcurso y terminación de las conexiones entrantes y salientes.
4. Este producto emplea ciertas funcionalidades más específicas, ayudándose de la creación de políticas o reglas, así como, inspeccionar, filtrar y proteger a organizaciones de ataques *DoS y IP/MAC spoofing*. Permitiendo el control de flujo de la red en cuestión y ofreciendo una amplia flexibilidad al cliente.
5. Según la regla establecida, Sophos Firewall mantendrá el transcurso normal del tráfico o desechará dicha petición.

2 OBJETO Y ALCANCE

6. El presente documento tiene como objeto detallar la integración segura del producto de Sophos Firewall, versión 20.0, en la infraestructura del cliente. Además, especifica la configuración necesaria para que el producto cumpla con los requisitos de la taxonomía en la que se ha cualificado este producto: CCN-STIC-140-D3 [REF1]**.**

7. Sophos Firewall, puede no solo actuar como cortafuegos, sino también, como *Router Gateway*. El alcance del producto es solo el SO de Sophos Firewall.

8. La evaluación del SO correspondiente a Sophos Firewall ha sido realizada mediante su *appliance hardware,* aunque también es posible descargar un appliance virtual. Las interfaces que proporciona el producto son las mencionadas en 1.INTRODUCCIÓN (CLI y Web).

3 ORGANIZACIÓN DEL DOCUMENTO

a) Apartado **4**. En este apartado se incluyen aspectos y recomendaciones a considerar, antes de proceder a la configuración del producto.

b) Apartado **5**. En este, se recogen recomendaciones a seguir durante la fase de preconfiguración del producto.

c) Apartado **6**. En esta sección se ofrecen las directrices necesarias para asegurar una configuración segura del producto.

d) Apartado **7**. En esta sección se incluyen las recomendaciones a seguir para la etapa de operación o mantenimiento del producto.

4 FASE PREVIA A LA CONFIGURACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

10. Las organizaciones interesadas en *Sophos Firewall,* pueden adquirir el producto a través de la página web principal de Sophos [REF3]**.** Acudiendo a la sección "*Products and Services*", al apartado de *"Network Security"* y hacer *click* en *"Next-gen Firewall"*, posteriormente, se debe acudir a la parte inferior de la web donde pone *"How to Buy"* y realizar click en *"Quote Request"* sobre la opción interesada. Donde se cumplimentará el formulario de contacto. En este formulario se expresará el interés de poseer alguno de los modelos disponibles, con los ajustes necesarios para cumplir con la normativa LINCE.

11. Tras la gestión contractual entre la parte interesada y Sophos, se podrá obtener el producto mediante dos métodos: De manera física o descargando Sophos Firewall desde el link indicado en [REF10]**.** A continuación, se explican los pasos que se siguen para la llegada del producto de manera física:

12. El equipo de Sophos hará efectiva la entrega a la dirección especificada por el cliente, aportando el número de seguimiento correspondiente al envío.

13. En su recepción, el cliente deberá poner atención al empaquetado verificando que este no ha sido manipulado durante su transporte. El receptor deberá comprobar que el contenido del paquete se corresponde con lo indicado en la etiqueta de la caja. Si se observa que la etiqueta está rota o no está, contacte con el proveedor del producto.

14. Una vez el producto se ha desempaquetado, compruebe que el modelo y número de serie que aparece en el propio producto coincide con el modelo y número de serie de la caja.

15. El producto que se entrega incluye el hardware y el firmware que compone el producto. Junto con el dispositivo, se incluye un impreso con la guía de seguridad y el listado de embalaje. Además, se proporciona acceso a las guías de instalación y configuración.

16. También, es posible acceder a los manuales y documentación técnica a través del enlace indicado en [REF4]**.**

17. Sophos mantendrá la comunicación con el cliente empleando direcciones de correo electrónico bajo el domino @sophos.com asegurando una comunicación directa y confiable.

4.2 ENTORNO DE INSTALACIÓN SEGURO

18. Sophos Firewall se distribuye como un producto listo para su configuración directa, de manera que el fabricante realiza la instalación inicial con las medidas de seguridad adecuadas.

19. Las primeras configuraciones iniciales deben realizarse desde la interfaz local. Seguidamente, se puede administrar el cortafuegos desde una interfaz web conectada a la misma red que el producto. Hay que asegurarse de cumplir ciertas medidas de protección física, para evitar problemas de seguridad durante las primeras configuraciones. Algunas consideraciones que tomar en cuenta son las siguientes:

    a) Utilizar credenciales fuertes para el acceso inicial, tal y como se indica en la sección 6.2.2.CONFIGURACIÓN DE ADMINISTRADORES.

b) Cambiar la contraseña predeterminada inmediatamente después del primer acceso.

c) Configurar el firewall para bloquear todos los puertos innecesarios.

d) Habilitar la autenticación de dos factores si está disponible.

e) Mantener actualizado el sistema operativo y las firmas de amenazas.

f) Limitar el acceso SSH solo a direcciones IP confiables si se utiliza este método.

4.3 REGISTRO Y LICENCIAS

20. Antes de llevar a cabo la integración del producto en la red del cliente, es necesario que se haya registrado el *appliance* proporcionado por Sophos, para obtener la licencia. Para ello se siguen los siguientes pasos:

    a) Crear una cuenta o iniciar sesión en el enlace referenciado en [REF5]**,** para después registrar el dispositivo, cumplimentando la información requerida en el formulario. Haciendo uso del número serial proporcionado por Sophos, para dicho *appliance*.

    b) Confirma el registro y activar la licencia de evaluación.

21. Además, se puede consultar más información sobre el licenciamiento acudiendo al enlace expuesto en [REF6]**.**

4.4 CONSIDERACIONES PREVIAS

22. Sophos Firewall proporciona múltiples opciones de instalación e integración como se hace referencia en previos apartados. Al ser un producto distribuido con el firmware instalado, no será necesario cumplir con unos requisitos hardware, ya que el producto se proporciona de forma compacta e integrada.

23. Asimismo, para el correcto funcionamiento de la interfaz web, es imprescindible contar con una conexión a internet estable y confiable.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

24. En esta sección, se van a detallar los componentes del entorno operacional que se comunican con el Sophos Firewall. Estos elementos son los siguientes:

    a) **Servidor *syslog*.** Un servidor *syslog* es un componente crucial para la recopilación y gestión centralizada de registros de eventos de la red. En este caso, recopila mensajes de registros del Sophos Firewall.

    b) ***Workstation* de gestión.** Un *workstation* de gestión es un equipo dedicado para la administración y monitoreo de sistemas y red. En este caso, se utiliza para configurar y administrar el Sophos Firewall.

c) **Componentes de red**. Estos componentes, son las redes que se comunican entre sí a través del Sophos Firewall.

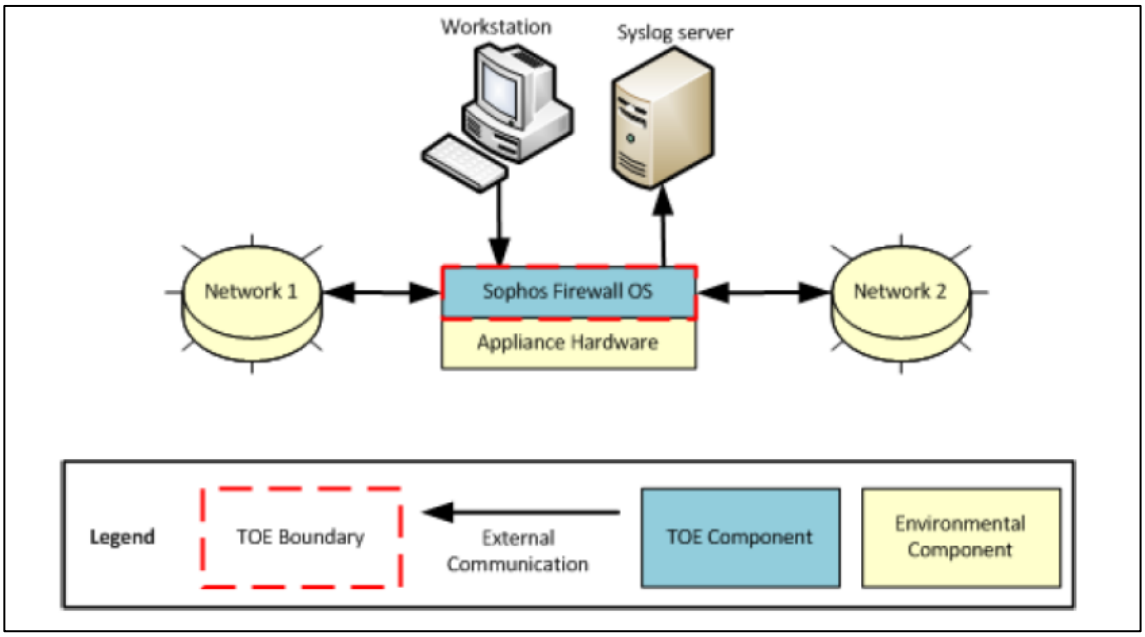

Figura 1.Descripción del entorno operacional.

5 FASE DE PRE-CONFIGURACIÓN

25. Una vez recibido Sophos Firewall, se procede a la fase de pre-configuración. Como se menciona anteriormente, este producto viene ya preinstalado en un *appliance* hardware. Se debe registrar previamente el dispositivo para obtener la licencia, tal y como se indica en la sección **4.3.REGISTRO Y LICENCIAS**. Además, se debe tener en cuenta la sección **4.FASE PREVIA A LA** .

26. Seguidamente, se siguen los siguientes pasos para iniciar la integración del producto en la red del cliente:

    1. Conecte el *appliance* a internet a través del puerto 2.
    2. Conecte el Workstation a Sophos Firewall, ya que desde aquí se va a llevar a cabo la integración. Para ello, se hará uso del puerto 1.
    3. En esta Workstation conectada al producto, abra el navegador y vaya hacia: *https://IP_SophosFirewall:Puerto*
    4. Acepte las condiciones de uso e inicie con la configuración.

Figura 2. Configuración inicial Sophos Firewall.

6 FASE DE CONFIGURACIÓN

27. Tras la preconfiguración del producto, se procede a su configuración de manera segura. Para ello, se siguen los siguientes pasos:

    a) Inserte la nueva contraseña de administrador de Sophos Firewall (La contraseña deberá seguir con los estándares establecidos por *CCN en la sección* **6.2.ADMINISTRACIÓN DEL PRODUCTO***).*

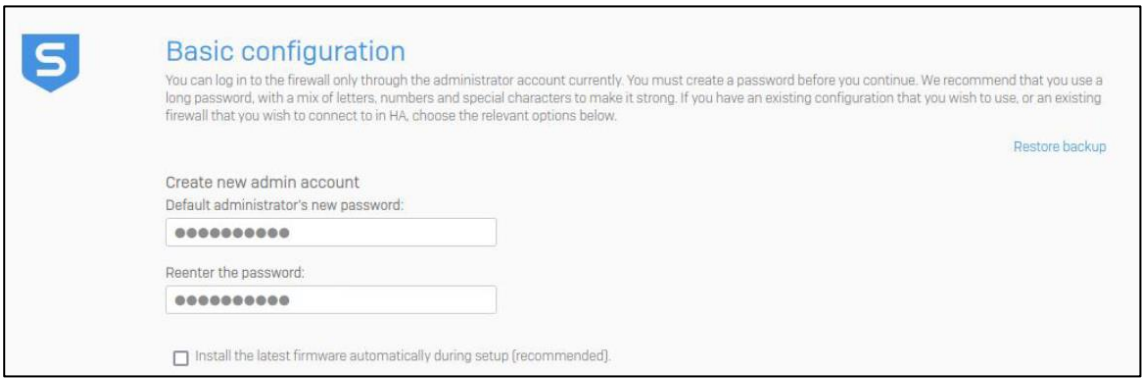

Figura 3. Configuración básica

    b) Haga *click* en continuar y seleccione el Time Zone acorde a su franja horaria. Se deberá indicar el área en la que se encuentra, de otra manera no aparecerán los logs, eventos y reportes monitorizados sincronizados.

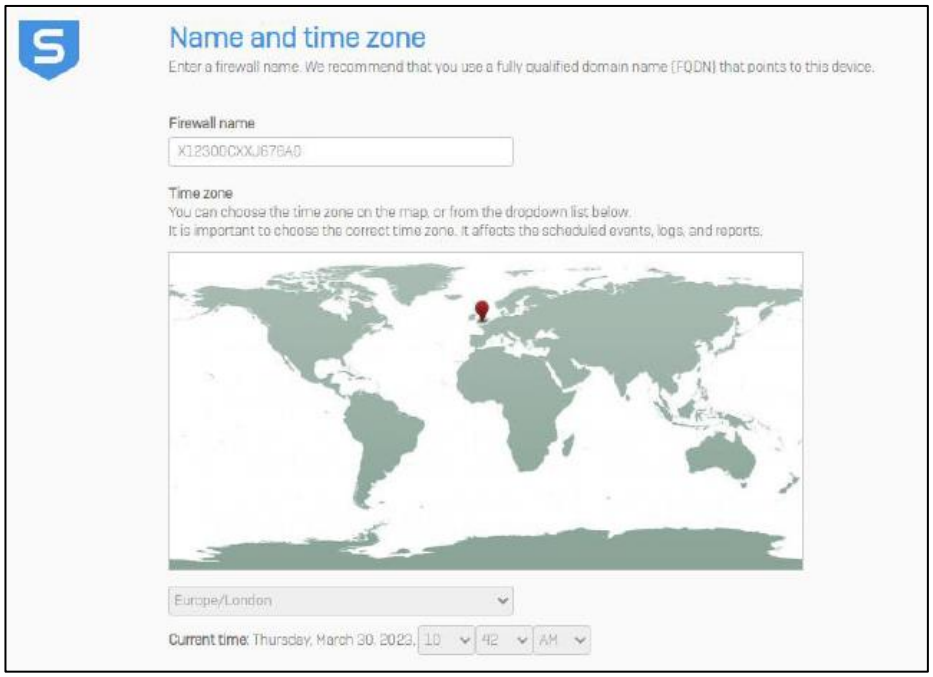

Figura 4. Nombre y zona horaria

c) Configure su red LAN, donde se ofrece la opción de añadir puertos, el modo de despliegue, así como, establecer su *LAN IP address* y la máscara de red o permitir el servicio DHCP si fuese necesario.

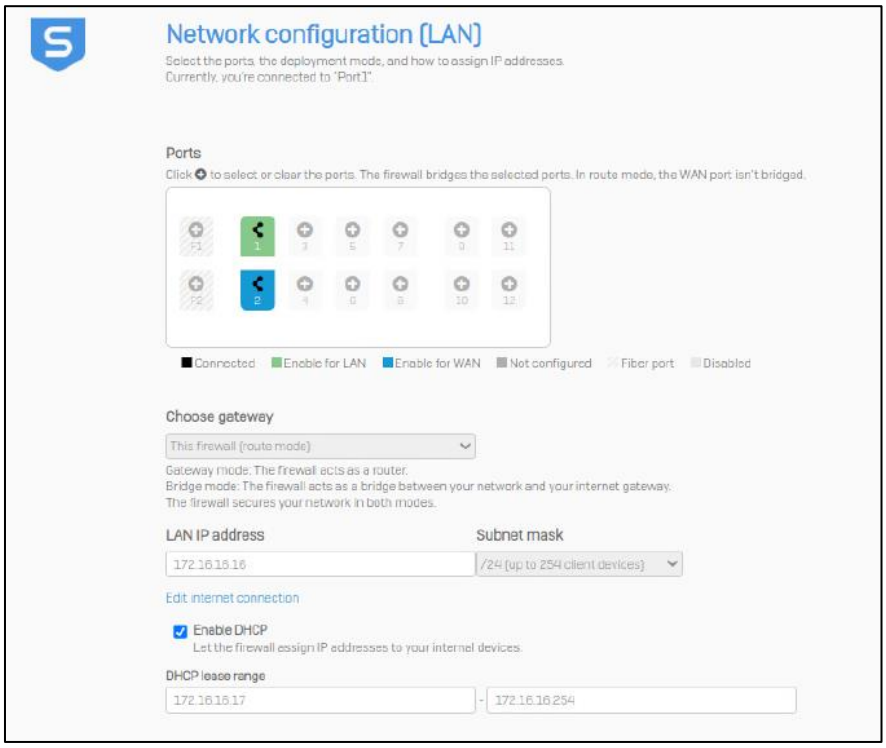

Figura 5. Configuración de red local

d) Sophos Firewall, también se ofrece la opción de configurar ciertos permisos para proteger a los usuarios cuando acceden a Internet. Seleccione los que vea convenientes para su uso.

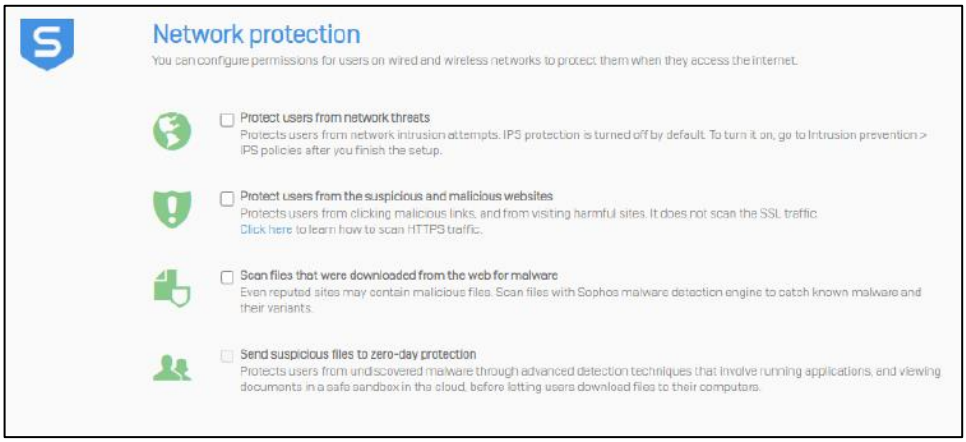

Figura 6. Protección de red

e) A continuación, se debe configurar la recepción de avisos o notificaciones vía email, para realizar *back-ups* por posibles problemas que pudieran ocurrir.

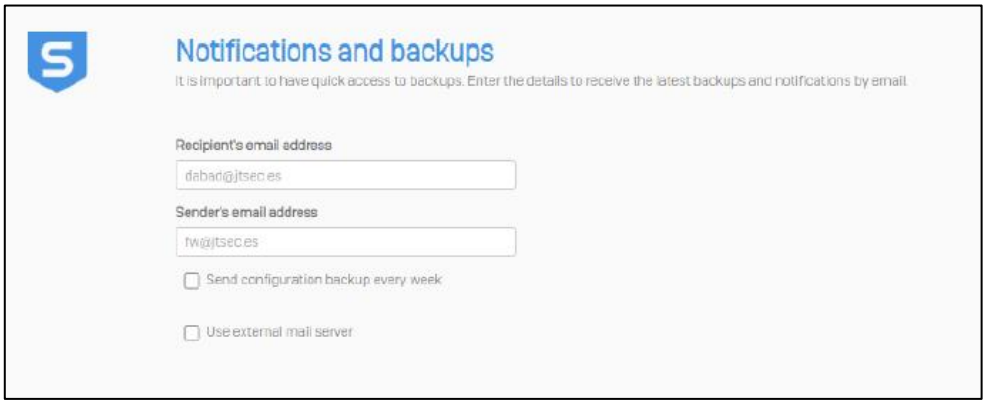

Figura 7. Notificaciones y backup

f) Por último, emerge una ventana sobre un resumen de las configuraciones realizadas. Si está de acuerdo y no existen errores, entonces, pulse finalizar.

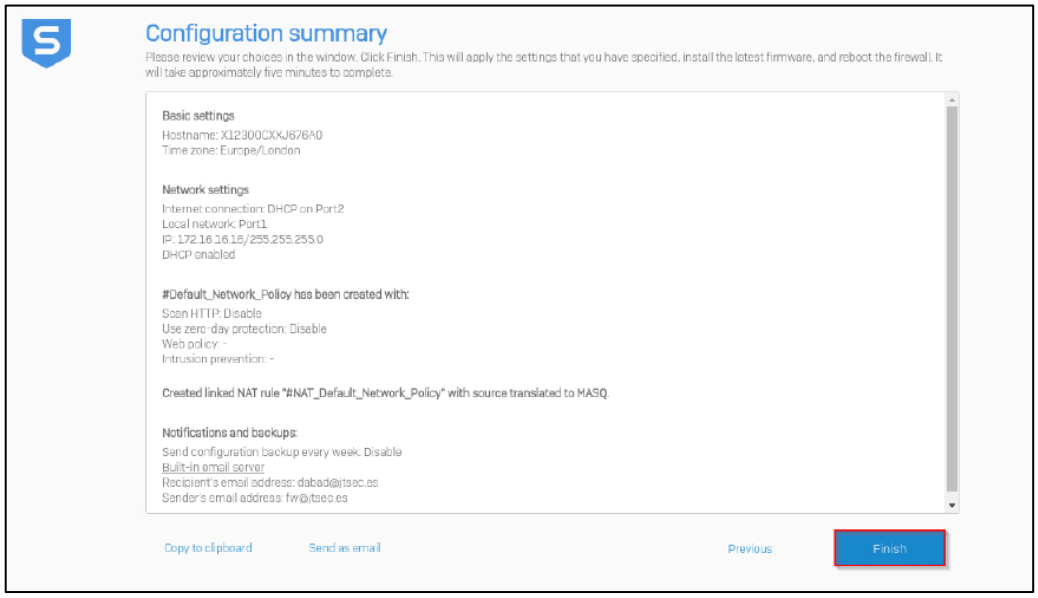

Figura 8. Resumen de la configuración

28. Se puede encontrar información adicional sobre la configuración de Sophos Firewall en el enlace referenciado [REF8].

6.1 MODO DE OPERACIÓN SEGURO

6.1.1 ACTIVA EL MODO LINCE

29. Inicie sesión, a través de la interfaz local CLI con el usuario y contraseña de administrador.
30. Acceda a la consola y ejecute el siguiente comando:

```
"system lince enable"
```

6.2 ADMINISTRACIÓN DEL PRODUCTO

31. El producto se administra localmente mediante acceso por consola, y remotamente, tanto por un portal de administración web, como por SSH.

6.2.1 ADMINISTRACIÓN LOCAL Y REMOTA

6.2.1.1 ADMINISTRACION POR SSH

32. Para utilizar la interfaz SSH que proporciona acceso remoto a Sophos Firewall, se deben modificar algunos mecanismos criptográficos:

33. Estos mecanismos deben cumplir con la guía CCN-STIC-807 [REF2]. A continuación, se indican algunos parámetros de longitud que se deben cumplir para garantizar la máxima seguridad requerida.

    a) DSA o RSA con claves de, al menos, 3072 bits de longitud.

    b) ECDSA con curvas P-256 o superior.

    c) Funciones Hash SHA-256 o superior.

    d) Cifrado AES-128 o superior.

    e) Grupos Diffie-Hellman 15, 16, 19, 20, 21, 28, 29 o 30.

    f) Elliptic Curve Diffie-Hellman P-256 o superior.

34. Para modificar estos parámetros en Sophos Firewall, debe realizar las siguientes configuraciones:

    a) Acceda a Sophos Firewall a través de SSH y navegue hacia *"Device Management" > Advanced.*

    b) Cambie el permiso de escritura, añadiendo el siguiente comando:

    c) "mount -no remount, rw/"

    d) Seguidamente, añada el siguiente comando para crear un *backup* del archivo */etc/ssh/sshd_config:*

    e) "cp /etc/ssh/sshd_config /etc/ssh/sshd_config.org"

    f) Edite el archivo */etc/ssh/sshd_config* usando un editor de texto.

    g) Cambie los mecanismos criptográficos y claves a los siguientes (para marcar los saltos de línea se han marcado en negrita las palabras que son el inicio de una nueva línea):

```
# Ciphers and keying
KexAlgorithms diffie-hellman-group16-sha512,diffie-hellman-group18-
sha512,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521
Ciphers aes128-gcm@openssh.com,aes256-gcm@openssh.com
MACs hmac-sha2-256,hmac-sha2-512
HostKeyAlgorithms ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-
nistp521
RekeyLimit 1G 3600
```

h) Guarde los cambios y salga del editor de texto.

6.2.1.2 ADMINISTRACIÓN POR HTTPS

35. La administración de Sophos Firewall se puede realizar de manera remota, mediante el protocolo HTTP sobre TLS. Este producto solo permite versiones de TLSv1.2 o superiores, en las que se hace uso de las siguientes cipher-suites reflejadas como recomendadas en la guía CCN-STIC-807 [REF2].

    a) TLS v1.2:

        i. TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

        ii. TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

        iii. TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256

    b) TLS v1.3:

        i. TLS_AES_256_GCM_SHA384

        ii. TLS_CHACHA20_POLY1305_SHA256

        iii. TLS_AES_128_GCM_SHA256

36. No se recomienda el uso de HTTP o protocolos como Telnet, ya que no aseguran una comunicación segura entre entidades.

6.2.2 CONFIGURACIÓN DE ADMINISTRADORES

37. Sophos Firewall proporciona varios aspectos de gestión relacionados a perfiles o roles creados dentro del producto. Un perfil separa las funcionalidades del cortafuegos en categorías de control de acceso para las cuales un usuario del producto puede habilitar acceso de sólo lectura, lectura-escritura o no proporcionar acceso directamente. Los perfiles por defecto que contiene Sophos Firewall son los siguientes:

    a) Administrador - Superusuario con todos los privilegios.

    b) Administrador de auditoría - Privilegios de lectura y escritura sólo para registros e informes.

    c) Administrador de Seguridad - Privilegios de lectura y escritura para todas las funciones excepto Perfiles de Acceso a Dispositivos (sólo lectura), Acceso a Dispositivos (sin privilegios) y Registros e Informes (sin privilegios).

38. Con los perfiles anteriores, Sophos Firewall permite a los usuarios administrar las siguientes funcionalidades:

    a) La gestión del SFP de Control de Flujo de Información de Tráfico, sus atributos de seguridad, y las reglas *"aceppt/drop/reject"*

    b) Establecer valores predeterminados restrictivos para el cortafuegos y debe ser configurado por un usuario con el perfil de *Security Admin o Administrator* para sobrescribir los valores predeterminados.

c) Configurar la protección de autenticación de usuario, esto incluye la funcionalidad relacionada con la gestión del manejo de fallos de autenticación, tiempos de espera de sesión y *banneo* de acceso.

d) Gestión de usuarios, esto incluye la funcionalidad relacionada con la gestión de los perfiles asociados a las cuentas de usuario.

e) Buscar o filtrar en el *Log Viewer*, esto incluye funcionalidad relacionada con la gestión de las vistas en el Visor de Registros.

39. Incluye funciones relacionadas con la gestión de permisos de acceso a servicios de administración y red, así como la definición y gestión de permisos de perfil de usuario administrador.

40. Se deben de tener en cuenta los siguientes aspectos, para cumplir con la normativa y la guía CCN-807 [REF2]:

a) **Configuración de la Política segura de contraseñas**. La política de contraseñas es configurable desde la interfaz web. En el enlace [REF13] se describe el proceso a seguir. Deberá cumplir con los siguientes requisitos mínimos:

i. Longitud mínima de la contraseña: doce (12) caracteres.

ii. Composición de la contraseña: letras mayúsculas, letras minúsculas, números y símbolos especiales. Recomendar el uso de los cuatro (4) grupos si el producto lo permite, y al menos un mínimo de tres (3) grupos.

b) **Configuración de los parámetros de sesión.** Deberá cumplir con los siguientes requisitos mínimos:

i. Tiempo de inactividad de las sesiones: 15 minutos por defecto, siendo configurable este parámetro. Es posible configurar la inactividad y bloqueo de sesión desde “System > Administration > Admin and user settings > Login security”.

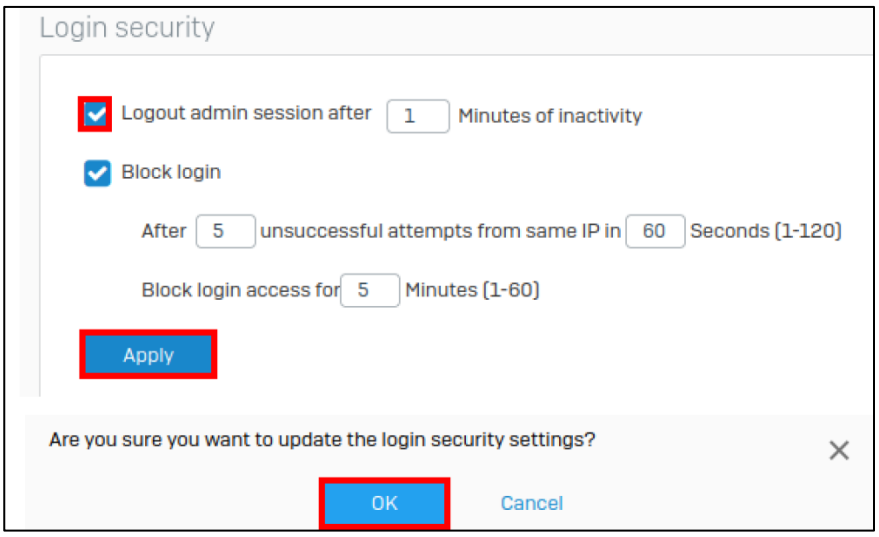

Figura.6. Configuración de seguridad para el inicio de sesión.

c) Número de intentos fallidos de inicio de sesión: tres 3 intentos.

d) Tiempo de bloqueo tras 5 intentos fallidos: cinco 5 minutos (configurable).

6.3 AUTENTICACIÓN

41. En esta sección, se describen algunas de las maneras de autenticación posibles para usuarios, sesiones SSH, servidores y demás componentes o servicios que requieran acceso a Sophos Firewall. Existen múltiples opciones de autenticación, según los protocolos y tecnologías usadas:

    a) Autenticación de usuarios, mediante credenciales locales (almacenadas en una base de datos interna) o mediante servidores externos abajo indicados.

    b) Autenticación de servicios mediante credenciales locales, servidores externos y/o certificados digitales.

    c) Autenticación entre componentes del producto y servidores o dispositivos externos, mediante certificados digitales.

    d) Autenticación de acceso SSH y acceso por consola mediante credenciales locales o servidores externos.

42. Sophos Firewall verifica que los usuarios que desean acceder al producto son usuarios autorizados. Hay que considerar, que se deben añadir los usuarios manualmente, mediante la interfaz web. Sin embargo, este producto también permite la integración de los siguientes servidores de autenticación:

    a) LDAP Server.

    b) Active Directory Server.

    c) Radius Server, entre otras opciones indicadas en la referencia [REF9]**.**

    d) Hay que recalcar el uso de parámetros seguros para la configuración de estos servidores de autenticación como: RADSEC, LDAPv3, o TLSv1.2.

43. Se debe minimizar el uso de clave precompartidas con los servicios y componentes que sea posible. Se recomienda el uso de certificados digitales y 2FA (*Two-Factor Authentication*), con objeto de maximizar la seguridad.

44. Si desea saber más sobre los mecanismos de autenticación de Sophos Firewall, por favor acceda al enlace referenciado en [REF9]**.**

6.4 CONFIGURA REGLAS FIREWALL

45. En orden de denegar, aceptar o filtrar cierto tipo de tráfico, Sophos Firewall ofrece la capacidad de crear algunas reglas. Para ello se pueden seguir los siguientes pasos:

    a) Iniciar sesión en Sophos Firewall y acudir a *"Protect > Rules and Policies".*

    b) Realizar Click en *"Add a Firewall Rule".*

    c) Posteriormente, se debe establecer la regla deseada.

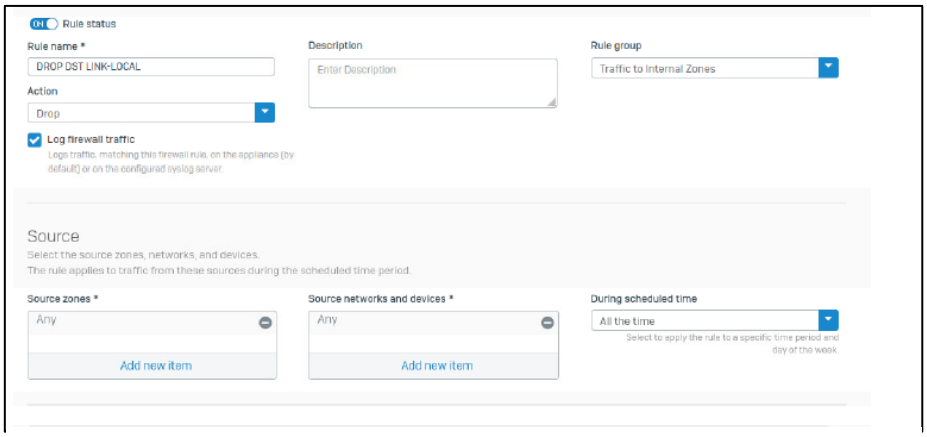

Figura. 1. Establecer reglas.

46. Además, se puede profundizar más en el funcionamiento de la creación de reglas firewall en el enlace referenciado en [REF9].

6.5 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

47. En esta sección se detallan todas las recomendaciones para la configuración segura de interfaces, puertos y servicios. Para más información sobre los ajustes que se van a describir el interesado deberá acudir al enlace referenciado en [REF7].

48. La configuración de las interfaces en Sophos Firewall es crucial para establecer una alta disponibilidad (HA) segura y eficiente. Los pasos principales son:

49. Selección de interfaces HA:

    a) Seleccionar una interfaz física, VLAN o LAG como enlace dedicado HA entre los dispositivos.

    b) Asegurarse de que la interfaz elegida no esté utilizada por otros servicios o funciones del firewall.

50. Configuración de interfaces:

    a) Configurar las interfaces en ambos dispositivos con direcciones IP estáticas en el mismo rango de subred.

    b) Establecer un nombre descriptivo para cada interfaz para facilitar la identificación.

51. Puertos de administración:

    a) Configurar los puertos de administración o gestión para acceder a las consolas web de los dispositivos primario y auxiliar. Para ello acuda al enlace referenciado en [REF8].

52. Tener en cuenta los puertos reservados por el sistema para evitar conflictos:

    a) Puertos TCP: 22, 80, 443, 4444, 8080, 8443

    b) Puertos UDP: 53, 123, 161, 162, 500, 4500. Esta información está detallada en el enlace referenciado en [REF11].

53. Requisitos adicionales:

    a) Activar el modo RSTP en el conmutador conectado a los puertos del firewall.

    b) Colocar los enlaces dedicados HA en la zona DMZ con SSH habilitado.

    c) Asegurar el mapeo puerto a puerto entre los dispositivos si se utiliza una interfaz LAG.

    d) Evitar usar interfaces que estén configuradas como puertos de administración o gestión.

    e) No compartir la misma IP en diferentes interfaces.

54. Siguiendo estos pasos y teniendo en cuenta las restricciones de puertos reservados, se garantiza una configuración de interfaces segura y eficiente para la alta disponibilidad en Sophos Firewall.

6.6 GESTIÓN DE CERTIFICADOS

55. Los certificados que se usan por defecto pueden no estar actualizados a las medidas de seguridad requeridas. Los certificados, deben estar configurados para soportar los algoritmos y funciones criptográficas de manera segura, cumpliendo así con las especificaciones de la guía CCN-STIC-807 [REF2]**.** Los parámetros seguros a configurar son los siguientes:

    a) RSA con claves de, al menos, 3072 bits de longitud.

    b) ECDSA con curvas P-256 o superior.

    c) DSA con claves de, al menos, 3072 bits de longitud.

    d) Funciones Hash SHA-256 o superior.

56. Para editar los parámetros usados por el certificado digital a modificar:

    a) Se debe, Iniciar sesión en el *dashboard* web de administración.

    b) Vaya seguidamente a "*System > Certificates".*

    c) Haga *click* en "*Certificate authorities"* y edite el "*Default*" CA.

    d) Cambie la longitud de clave a 4096 y haga *click* en guardar.

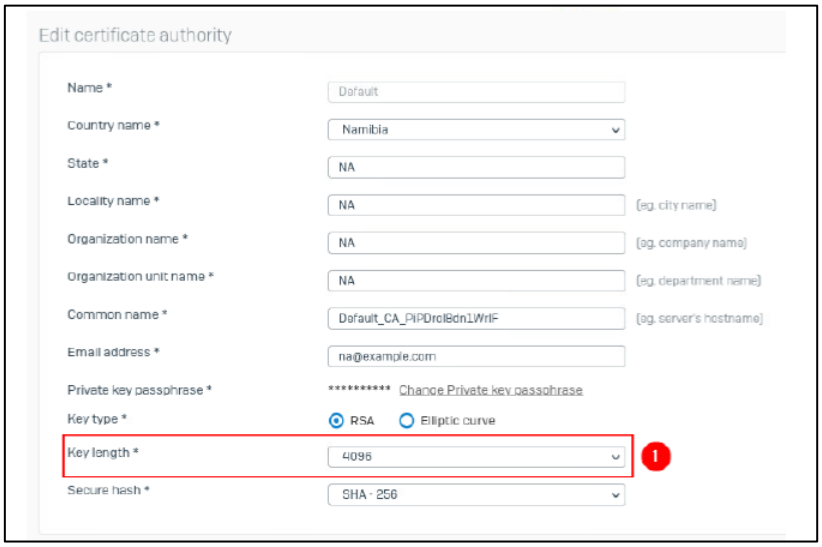

Figura. 2.Cambiar el certificado por defecto.

57. A continuación, se va a detallar el procedimiento para la configuración de certificados. Primero, veremos la generación de solicitudes de certificado (CSR):

    a) Sophos Firewall permite generar CSR directamente desde la interfaz de administración.

    b) Se puede especificar el algoritmo criptográfico y la longitud de la clave durante este proceso.

58. Importación del certificado del servidor:

    a) Una vez obtenido el certificado firmado por una Autoridad Certificadora (CA), se puede importar en Sophos Firewall.

    b) El sistema verifica automáticamente la validez y compatibilidad del certificado.

59. Importación de certificados de CAs:

    a) Sophos Firewall permite importar certificados raíz y de CA intermedios.

    b) Esto es crucial para establecer cadenas de confianza válidas.

60. Para obtener información más detallada, visite el enlace referenciado en [REF9].

6.7 SINCRONIZACIÓN

61. Se puede realizar la funcionalidad de sincronización, haciendo uso del servicio NTP. En caso de que sea posible, active la autenticación si se requiere. La configuración de la sincronización debe ser empleada de manera segura, para ello se puede seguir el enlace que se muestra en la siguiente referencia [REF9].

62. La configuración de dicho servicio se hará mediante la interfaz web de administración, acorde al uso recomendado del mismo en el presente procedimiento de uso.

63. NTP está deshabilitado si no hay servidores de tiempo configurados y se podrá ajustar el *Time zone* manualmente.

6.8 ACTUALIZACIONES

64. Es esta sección, se va a realizar una descripción mediante referencias a la guía de cómo el producto realiza las actualizaciones de firmware, software, servicios, etc. de forma segura.

65. Se debe mantener el producto actualizado, sobre todo en lo que respecta a parches de seguridad. Para realizar la actualización, se deberá ir a *"System > Backups & firmware > Firmware"*. Donde se podrá ver la versión actual y "checkear" qué actualización está activa o se puede realizar autenticando esta misma.

66. En la siguiente tabla se ven los perfiles posibles, para poder realizar actualizaciones:

PERFIL	Permiso para Actualizar
Administrador	**SI**
Cypto Admin	**NO**
Security Admin	**SI**
Audit Admin	**NO**
HAProfile	**NO**

Tabla 1.Perfiles con permisos para actualizar.

6.9 AUTO-CHEQUEOS

67. Sophos Firewall realiza actualizaciones automáticamente de forma predeterminada. Acuda a la siguiente referencia, para encontrar más información [REF9].

68. El producto permite actualizar definiciones de patrones para componentes, firmas, clientes y dispositivos.

6.10 ALTA DISPONIBILIDAD

69. En Sophos Firewall, se pueden establecer nodos como HA (High Availability), para aumentar la redundancia y minimizar el tiempo de *back-up*. Se puede encontrar más información en el enlace referenciado en [REF7].

70. Para ofrecer una disponibilidad alta en la red, se piden unos requisitos hardware. Además, se detallan los modos activo y pasivo, así como el despliegue en el enlace referenciado en [REF7].

71. Para conseguir una alta disponibilidad, en la sección **6.5.CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS** se indica una configuración de puertos (HA), Indicar en este documento los parámetros de configuración necesarios para una configuración segura.

6.11 AUDITORÍA

6.11.1 REGISTRO DE EVENTOS

72. Sophos Firewall es capaz de generar información de auditoría, registrando los siguientes tipos de logs tanto localmente, como enviándolos a un servidor remoto *syslog*:

a) Inicio de sesión y cierre de sesión de los usuarios registrados.

b) Cambios de configuración en el servidor remoto de auditoría.

c) Creación, modificación y eliminación de usuarios.

d) Cambios de administrador en el tiempo.

e) Inicio de actualizaciones de manera manual.

f) Generación, importación, cambios y eliminación de claves criptográficas.

73. Sophos Firewall también sobrescribe las entradas más antiguas de los registros de eventos cuando su almacenamiento está alcanzando su límite máximo.

74. Para seleccionar donde se envían los logs, se debe realizar *click* en "Log Setting" tal y como se indica en el enlace referenciado en [REF9]**.**

75. A continuación, se indica el formato de los logs que se registran:

FIELD	DESCRIPTION
timestamp	Fecha (yyyy-mm-dd (hh:mm:ss) de cuando el evento sucedió.
messageid	Identificación de mensaje (solo para logs locales).
log_type	Tipo de evento.
log_component	Componente responsable.
log_subtype	Subtipo de evento ocurrido.
status	Estado del log.
user	Nombre del usuario del log.

Tabla 2. Formato de logs

6.11.2 ALMACENAMIENTO LOCAL

76. En esta subsección se va a explicar cómo funciona el almacenamiento local de registros de auditoría en el producto:

77. Este producto proporciona una funcionalidad para ver los logs desde la interfaz web llamado "*Log Viewer*". Más información de cómo funciona disponible en el enlace referenciado en [REF9]**.**

78. Los registros de logs se almacenan de manera local en la siguiente ruta *"/var/eventslogs/backup.db".*

6.11.3 ALMACENAMIENTO REMOTO

79. El almacenamiento remoto se configura mediante el envío de registros a un servidor remoto syslog. Deberá utilizarse siempre un protocolo seguro para el envío de los registros (Por ejemplo, TLSv1.2 o IPsec). Para ello, seguimos los siguientes pasos:

80. Para una conexión segura entre Sophos Central y el *syslog* server si se configura, haz uso del enlace referenciado en [REF9].

81. Se ofrece más información sobre la configuración en el siguiente enlace referenciado en [REF12].

6.12 BACKUP

82. Es importante la realización *back-ups periódicas*, para disponer de una copia de seguridad de los datos y configuraciones realizadas sobre el producto.

83. Las copias de seguridad contienen toda la configuración del cortafuegos y están cifradas. Puede guardar las copias de seguridad en el cortafuegos, utilizar FTP para guardarlas en un servidor o enviarlas por correo electrónico. También puede programar una copia de seguridad automática o realizarla manualmente. Hay más información en el enlace referenciado en [REF9].

7 FASE DE OPERACION

84. Una vez completada la integración y configuración del sistema, es crucial implementar los siguientes pasos durante las fases de funcionamiento y mantenimiento:

a) Inspecciones rutinarias del hardware y software para garantizar que no se haya incorporado ningún componente o programa no autorizado.

b) Verificaciones sistemáticas del firmware activo, así como, su integridad. Estas comprobaciones se realizan con el propósito de asegurar que el firmware está libre de malware.

c) Implementación periódica de actualizaciones y parches de seguridad para mantener una configuración segura y protegida.

d) Realización regular de back-ups y almacenamiento centralizado de los datos.

e) Transmisión de registros de auditoría a un servidor *syslog* remoto, así como copias de seguridad criptográficas.

8 REFERENCIAS

[REF1] Taxonomía del Producto: Cortafuegos

[REF2] Guía CCN-STIC-807

[REF3] Web oficial del fabricante

[REF4] Documentación oficial del fabricante

[REF5] Portal de registro de Licencia

[REF6] Documentación sobre las licencias de Sophos

[REF7] *High Availability help*

[REF8] *Start Up Help*

[REF9] *Administrator Help*

[REF10] *Download Installers*

[REF11] *User Portal Help*

[REF12] *Syslog File guide*

[REF13] Configuración de la política de contraseñas

9 ABREVIATURAS

ENS	Esquema Nacional de Seguridad
SFP	Small Form-Factor Pluggable
DoS	Denial of Service
IP	Internet Protocol
MAC	Media Access Control
DMZ	eDelimitarized Zone
LAN	Local Area Network
CCN	Centro Criptológico Nacional
LINCE	Certificación Nacional Esencial de Seguridad
SSH	Secure Shell
QR	Quick Response
DHCP	Dynamic Host Configuration Protocol
CLI	Command Line Interface
UDP	User Datagram Protocol
TCP	Transmission Control Protocol
CA	Certificate Authority
RADSEC	RADIUS over DTLS
LDAP	Lightweight Directory Access Protocol
TLS	Transport Layer Security
HTTPS	Hypertext Transfer Protocol Secure
RSA	Rivest-Shamir-Adleman
AES	Advanced Encryption Standard
SHA	Secure Hash Algorithm
HA	High Availability
VLAN	Virtual Local Area Network
LAG	Link Aggregation Channel
CSR	Certificate Signing Request
NTP	Network Time Protocol
FTP	File Transfer Protocol
RSTP	Rapid Spanning Tree Protocol

PUBLICACIONES DE DEFENSA

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