centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1453

Procedimiento de Empleo Seguro
OPNsense Business Edition

Octubre 2025

MINISTERIO DE DEFENSA

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-26-126-6

Fecha de Edición: Octubre de 2025

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.05.05 10:28:08 +02'00'

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. OPNsense es una plataforma *software* de enrutamiento y cortafuegos basada en un Sistema Operativo BSD de código abierto fortificado, fácil de usar e implantar.

2. Se trata de un cortafuegos con estado, que hace un seguimiento del estado de las conexiones de red que viajan a través de él, permitiendo agrupar reglas de filtrado de tráfico de red por categoría.

3. Como cortafuegos, cuenta con las siguientes características básicas:

   - Protección contra tráfico procedente de redes no confiables hacia redes confiables, limitando el acceso de paquetes originados en las primeras de acuerdo a una/s política/s aplicada/s.
   - Restricción del tráfico originado en redes confiables hacia redes no confiables, especificando los protocolos/dispositivos/usuarios permitidos conforme a la/s política/s aplicada.

4. Siendo un cortafuegos con inspección de estados (*Stateful Firewall*), permite usar alias para identificar fácilmente y de manera comprensible orígenes, destinos y puertos empleados en las comunicaciones. Las reglas de acceso pueden desactivarse, agruparse por categoría y usarse en rangos definidos de tiempo, indicando la acción a tomar sobre cada tipo de tráfico. OPNsense soporta los protocolos TCP, UDP e ICMP sobre IPv4 e IPv6.

5. El producto permite a un usuario con rol de administrador gestionar de manera centralizada el producto, así como las necesidades de seguridad de la red que protege, previa autenticación en el sistema, y cumpliendo las pertinentes políticas de seguridad.

6. El producto ofrece la posibilidad de establecer comunicaciones seguras mediante los protocolos SSHv2 y HTTPS con otras entidades autorizadas, entre ellas servicios que permiten la actualización, protección de la integridad y autenticidad del mismo durante su instalación y ciclo de vida.

7. Dispone de distintos tipos de informes de auditoría, relativos a los paquetes de datos que atraviesan el dispositivo, la calidad de la conexión, métricas de rendimiento del sistema, flujos de tráfico y usuarios conectados vía VPN. Dichos informes permiten la detección y trazabilidad de cualquier evento que ocurre durante la utilización del producto.

8. Además, el producto dispone de funcionalidades adicionales, tales como:

   - Gestión de tráfico (*Traffic Shaping*), para controlar el tráfico de red y garantizar el rendimiento, la baja latencia y el ancho de banda utilizable, permitiendo introducir retardos en el procesamiento de paquetes que cumplan ciertos criterios.
   - Portal cautivo (*Captive Portal*), que fuerza a los usuarios a autenticarse como paso previo al acceso a la red.
   - Alta disponibilidad/Tolerancia a fallos (*High Availability/Hardware Failover*) a través del protocolo *CARP* [REF1], permitiendo un clúster en modo activo/pasivo.
   - Detección y Prevención de Intrusión (*Intrusion Detection & Prevention*) usando Suricata [REF2] y Netmap [REF3], permitiendo la inspección profunda de paquetes con un alto rendimiento y bajo consumo de CPU.
   - Red Privada Virtual (Virtual Private Network) mediante los programas/protocolos IPSEC, *OpenVPN, OpenConnect y Wireguard*.

9. Dichas funcionalidades adicionales no se encuentran bajo el alcance de la evaluación.

2 OBJETO Y ALCANCE

10. El objeto del presente documento es servir como guía para realizar una instalación, configuración y operación segura del cortafuegos *software* **OPNSense Business Edition** (versión comercial). Se recomienda consultar la última versión cualificada del producto.

11. Este producto ha sido cualificado e incluido en el Catálogo de Productos y Servicios STIC (CPSTIC) del Centro Criptológico Nacional para categoría ENS ALTA en la familia "Cortafuegos". Se recomienda consultar la versión cualificada en cada momento.

3 ORGANIZACIÓN DEL DOCUMENTO

- Apartado 4. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto
- Apartado 5. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.
- Apartado 6. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.
- Apartado 7. Este apartado contiene la documentación a la que se ha hecho referencia a lo largo de este documento.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

12. El producto es una plataforma software descargable para la arquitectura amd64 desde la dirección https://opnsense.org/download/ [REF4]. La descarga y verificación de la misma se realizarán conforme a lo indicado en https://docs.opnsense.org/manual/install.html [REF5], apartado "*Download and verification*".

13. Los tipos de imágenes descargables son:

    - DVD, imagen ISO con sistema en vivo, con VGA y soporte UEFI.
    - VGA, imagen ISO con sistema en vivo, con VGA y soporte UEFI.
    - SERIAL, imagen USB con sistema vivo, consola seria (115200) y soporte UEFI.
    - NANO, imagen preinstalada para dispositivos USB con tamaño al menos de 4GB, para usar en dispositivos embebidos con consola serial (115200) y soporte alternativo de VGA.

14. La herramienta OpenSSL es empleada para llevar a cabo la verificación de ficheros. Son necesarios 4 ficheros para llevar a cabo la verificación:

    - La imagen ISO comprimida en .bzip (*<filename>.iso.bz2*)
    - El fichero de suma de comprobación (*checksum*) en SHA-256 (*<filename>.sha256*)
    - El fichero de firma (*<filename>.sig*)
    - La clave pública, empleada por Openssl (*<filename>.pub*)

15. Estos ficheros pueden ser descargados desde uno de los mirrors de descarga. Para descargar dichos ficheros

    - Ir a la página de descarga de OPNSense [REF4].
    - Una vez seleccionado el *mirror* de descarga, hacer *click* derecho en el botón de descarga y hacer click en "*open new tab*".
    - Aparecerá una ventana emergente preguntando si se desea descargar la imagen del producto. Seleccionar la opción "no".
    - Eliminar el nombre de fichero tras el último "*/*" en la URL, y presionar ENTER. Esto redirigirá al listado del directorio de descargas.
    - Descargar los ficheros mencionados en el punto anterior.

16. La clave pública es necesaria para llevar a cabo la verificación de la imagen descargada. Se recomienda que dicha clave coincide con la clave pública proporcionada por las distintas fuentes alternativas disponibles.

17. A continuación, se introduce un conjunto de fuentes alternativas desde las que obtener el fichero de clave pública:

    - https://pkg.opnsense.org/releases/mirror/README
    - https://forum.opnsense.org/index.php?board=11.0
    - https://opnsense.org/blog/
    - https://github.com/opnsense/changelog/tree/master/community
    - https://pkg.opnsense.org/

18. Una vez descargados los ficheros necesarios, y comprobada la validez de la clave pública, habrá que llevar a cabo la comprobación de la integridad de la imagen descargada, mediante el comando:

```
#openssl sha256 OPNsense-<filename>.<extensión>
```

19. Habrá que comparar el checksum obtenido tras la ejecución de este comando con los valores proporcionados por el fichero *OPNsense-<version>-OpenSSL-checksums-amd64.sha256*. Si los valores no coinciden, habrá que volver a descargar la imagen. Este checksum viene indicado en la página de descarga del producto.

20. Si la comprobación de la suma de comprobación (checksum) es exitosa, ejecutar los siguientes comandos:

```
#openssl base64 -d -in <filename>.sig -out /tmp/image.sig
#openssl dgst -sha256 -verify <key>.pub -signature /tmp/image.sig
<image>.img.bz2
```

21. En caso de haber descargado la imagen de instalación en formato .iso, será necesario cambiar en el segundo comando, el formato "sig" por "iso".

22. Si el resultado de la ejecución del segundo comando es "*Verified OK*", la imagen habrá sido verificada con éxito.

4.2 ENTORNO DE INSTALACIÓN SEGURO

23. Se deberán cumplir las medidas de seguridad físicas y lógicas de aplicación a los sistemas donde se desea desplegar el software.

24. Estas medidas de seguridad deberán garantizar que los sistemas donde se despliega el software se encuentren de forma protegida, permitiendo el acceso solamente a personal autorizado (considerando únicamente al administrador como confiable).

4.3 REGISTRO Y LICENCIAS

25. Siendo *software* libre, se descarga desde la dirección https://opnsense.org/download/ [REF4] sin necesidad de registro.

26. El licenciamiento puede consultarse en la dirección https://docs.opnsense.org/legal.html [REF6], siendo una licencia de tipo BSD 2-Clause simplificada.

4.4 CONSIDERACIONES PREVIAS

27. Como aspectos previos a tener en cuenta antes de la instalación, respecto a las **plataformas hardware soportadas**, requerimientos hardware, impacto de las funciones habilitadas respecto al rendimiento y capacidad de gestión del tráfico respecto al hardware, estos pueden ser consultados en el siguiente enlace: https://docs.opnsense.org/manual/hardware.html [REF7].

28. Es necesario indicar que el hardware en el que se instale el producto debe ser capaz de soportar Sistemas Operativos con arquitecturas de 64 bits.

29. En cuanto a detalles respecto a instalaciones virtualizadas, en entornos VMWare *ESXi/Xen/HyperV/KVM/AWS/Azure* y entornos hospedados, estos pueden ser

consultados en el siguiente enlace: *https://docs.opnsense.org/manual/virtuals.html* [REF8].

5 FASE DE INSTALACIÓN

30. Es posible elegir entre instalaciones completas o instalaciones embebidas, tal y como se recoge en el siguiente enlace: *https://docs.opnsense.org/manual/install.html* [REF5].
31. Asimismo, es posible descargar el software de diversas ubicaciones espejo en Internet y verificar el mismo mediante una suma de comprobación y la clave pública OpenSSL de verificación del espejo desde donde se lleva a cabo la descarga (ver sección 4 FASE PREVIA A LA INSTALACIÓN).
32. Se debe preparar el dispositivo donde se desea instalar el software, pudiendo ser este físico o virtualizado. Debe contar con acceso por consola, ya sea mediante teclado y monitor o a través de un puerto serie.

5.1 PREINSTALACIÓN EN ENTORNO FÍSICO

33. Una vez descargada y verificada la imagen de instalación, se tiene que arrancar el equipo físico seleccionando el TOE como medio de arranque.
34. Tras esto, las instrucciones de instalación se encuentran en la sección 5.3 INSTALACIÓN DEL TOE.

5.2 PREINSTALACIÓN EN ENTORNO VIRTUALIZADO

35. Una vez descargada y verificada la imagen de instalación, se tiene que abrir el entorno de virtualización deseado y seleccionar la opción de crear una nueva máquina virtual. A continuación, se detallan los pasos para el proceso de instalación general:
    - Seleccionar la ISO del TOE como medio para arrancar la máquina virtual.
    - Dar un nombre a la máquina virtual.
    - Establecer 30 GB para el espacio del disco.
    - Establecer 1 GB de memoria RAM.
    - Además, añadir los adaptadores de red necesarios para las necesidades de la red.
    - Seleccionar cerrar.
    - Seleccionar finalizar.
36. Tras esto, las instrucciones de instalación se encuentran en la sección 5.3 INSTALACIÓN DEL TOE.

5.3 INSTALACIÓN DEL TOE

37. Luego de seguir los pasos descritos en las secciones anteriores dependiendo del tipo de despliegue, a continuación, se detallan los pasos necesarios para instalar el TOE:
    - Esperar a que el TOE se inicie.
    - Para instalar el TOE, iniciar sesión con el usuario “instaler” y autenticarse con la contraseña “opnsense”.
    - Seleccionar la distribución del teclado.

- Indicar “Continue with…”
- Seleccionar “Install (UFS)” y presionar Enter.
- Seleccionar “stripe” y presionar Enter.
- Seleccionar el disco virtual y presionar OK.
- Seleccionar Yes y presionar Enter.
- Seleccionar “Change root password” y presionar OK.
- Definir una nueva contraseña para el usuario *root*. La contraseña deberá cumplir con la siguiente política de contraseñas:
  - **i.** Debe contener una longitud mínima de 12 caracteres.
  - **ii.** Debe contener 3 de los siguientes 4 tipos de caracteres: mayúsculas, minúsculas, números y caracteres especiales ("!", "@", "#", "$", "%", "^", "&", "*", "(", ")")
- Seleccionar “Complete Install” y seleccionar *OK*.
- Esperar a que se reinicie el TOE
- Navegar hacia la interfaz web del TOE.
- Iniciar sesión con las credenciales del usuario *root*.
- Seguir el asistente de configuración, seleccionar *Next*.
- Dar un nombre y un dominio al TOE y seleccionar *Next*.
- Establecer los servidores NTP y la fecha del sistema. En este caso los servidores NTP son los que se ofrecen por defecto. Seleccionar *Next*.
- Dejar por defecto los parámetros de configuración relacionados con la interfaz WAN y seleccionar *Next*.
- Dejar por defecto los parámetros de configuración relacionados con la interfaz LAN y seleccionar *Next*.
- Establecer una nueva contraseña del usuario *root* si no se ha cambiado anteriormente. La contraseña deberá cumplir con la política de contraseñas previamente declarada en el paso 48.
- Seleccionar en la opción de recargar y aplicar los cambios.

38. Para más información sobre cómo llevar a cabo la instalación en dispositivos hardware, se recomienda consultar el siguiente enlace: https://docs.opnsense.org/manual/hardware.html [REF7]
39. Para más información sobre cómo llevar a cabo la instalación en dispositivos virtualizados, se recomienda consultar el siguiente enlace: https://docs.opnsense.org/manual/virtuals.html [REF8]
40. En caso de que el TOE se provea en una versión distinta a la versión cualificada, se tienen que seguir los siguientes pasos:
    - Iniciar sesión en la interfaz web con el usuario *root*.
    - Ir a `System > Firmware > Settings` y habilitar la opción “Advanced mode”.

- En el parámetro "*Flavour*", se tiene que indicar "<Versión proporcionada>/MINT/<Versión cualificada>/latest" e introducir la clave de suscripción, donde se deben rellenar los parámetros "<Versión proporcionada> y <Versión cualificada> conforme corresponda.
- Ir a la sección de "*Status*" y seleccionar la opción "*Check for updates*".
- Seleccionar "*Update*".
- Esperar a que se instale la actualización.

6 FASE DE CONFIGURACIÓN

41. La presente sección describe paso a paso las distintas configuraciones que deben realizarse para que el producto actúe en su modo de operación seguro.

6.1 AUTENTICACIÓN

42. Los mecanismos de autenticación que utiliza son:

    - Autenticación de usuarios, mediante credenciales locales (almacenadas en una base de datos interna).
    - Autenticación con servidores o dispositivos externos a través del protocolo TLS (en sus versiones 1.2 o 1.3), mediante certificados digitales.

43. El sistema soporta autenticación de doble factor, para acceder a la interfaz gráfica (GUI) de gestión. Por tanto, deberá utilizarse el doble factor de autenticación siempre que sea posible. Se realiza mediante un TOTP, soportando el RFC 6238. Pueden consultarse los detalles en el siguiente enlace: *https://docs.opnsense.org/manual/two_factor.html* [REF9].

6.2 ADMINISTRACIÓN DEL PRODUCTO

6.2.1 ADMINISTRACIÓN LOCAL Y REMOTA

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

45. Se debe reforzar la seguridad en el acceso a la gestión del sistema a través de la interfaz gráfica de usuario de la siguiente forma:

    - Iniciar sesión en la interfaz web con el usuario *root*.
    - Navegar hasta `System > Settings > Administration`.
    - En la sección de Web GUI, seleccionar el menú desplegable de *SSL Ciphers* y seleccionar las siguientes:
        - TLS_AES_128_GCM_SHA256
        - TLS_AES_256_GCM_SHA384
        - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
        - TLS_CHACHA20_POLY1305_SHA256
        - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
        - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

46. Se debe reforzar la seguridad en el acceso a la gestión del sistema a través de SSH de la siguiente forma:

    - Iniciar sesión a través de la interfaz web con el usuario *root*.
    - Navegar hasta System > Settings > Administration.
    - En la sección *Secure Shell*, seleccionar el menú desplegable para las siguientes secciones y seleccionar los parámetros criptográficos especificados a continuación:
        - SSH Key Exchange Method

        - diffie-hellman-group16-sha512
        - diffie-hellman-group18-sha512
        - ecdh-sha2-nistp256
        - ecdh-sha2-nistp384
        - ecdh-sha2-nistp521
    - SSH Encryption Algorithms
        - aes128-ctr
        - aes192-ctr
        - aes256-ctr
    - SSH Public Key Algorithm
        - ecdsa-sha2-nistp256
    - SSH MAC Algorithm
        - hmac-sha2-256
        - hmac-sha2-512

47. Se debe reforzar la seguridad cuando se establece una conexión con un servidor syslog de la siguiente forma:

    - Iniciar sesión en la CLI con el usuario *root*.
    - Editar el archivo: /etc/local/opnsense/service/templates/OPNsense/Syslog/syslog-ng-destinations.conf
    - En los parámetros de red, dentro de los parámetros de TLS, añadir las siguientes líneas:

```
ssl-options(no-sslv2, no-sslv3, no-tlsv1, no-tlsv11) cipher-
suite("ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-
SHA256s:TLS_AES_256_GCM_SHA384:TLS_AES_128_GCM_SHA256:TLS_AES_128_GCM
_SHA256:TLS_CHACHA20_POLY1305_SHA256:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-CCM:ECDHE-
ECDSA-AES128-CCM")
```

    - Guardar el archivo.

48. Es necesario deshabilitar el acceso al usuario *root* a la interfaz CLI a través de SSH, permitiendo al usuario *root* acceder a la CLI solamente de forma local. Para ello, mediante la interfaz gráfica de usuario, en la ruta `Sysem > Settings > Administration > Secure Shell`, se debe desmarcar la opción "*Permit Root Login*".

6.2.2 CONFIGURACIÓN DE ADMINISTRADORES

49. A continuación, se enumeran los diferentes tipos de cuentas o roles que admite el producto:

    - Cuenta de usuario root, con acceso total al sistema.
    - Grupo de "super usuarios" admins, con acceso completo a todas las páginas de la interfaz web de administración. Este acceso es configurable, permitiendo la creación de grupos nuevos, y elegir las partes de la web de administración donde tiene acceso cada grupo de usuarios.

50. A través del menú `System > Access` es posible gestionar tanto usuarios (Users) como asociarlos a grupos (Groups), para definir las partes de la web de gestión a las que tendrán acceso. Se puede consultar la dirección https://docs.opnsense.org/manual/how-

tos/user-local.html [REF10] con instrucciones al respecto y cómo reforzar la seguridad de dichas cuentas.

51. Se deben **crear cuentas alternativas de administración** distintas de *root*, con las que operar normalmente. Se les debe asignar el mínimo privilegio posible, en función del nivel requerido de administración sobre el sistema.

52. Es posible establecer una política de contraseñas para reforzar la seguridad de estas mismas. Se deben seguir los siguientes pasos para configurar la política de contraseñas:

    - Iniciar sesión en la Web GUI.
    - Navegar hacia `System > Access > Servers`.
    - Seleccionar la opción de *Local Database*.
    - Configurar los siguientes valores como se indica:
        - **Policy:** Activar las restricciones de la política de contraseñas.
        - **Length:** Mínima longitud requerida, establecer 12 caracteres.
        - **Complexity:** Habilitar las verificaciones de contraseñas complejas.

53. Es posible configurar y modificar el tiempo de inactividad de cada interfaz, para ello deben seguirse los siguientes pasos:

    - Iniciar sesión en la Web GUI.
    - Navegar hasta `System > Settings > Administration`.
    - En el campo *Session Timeout* (para la Web GUI), introducir el valor "5".
    - En el campo *Inactivity Timeout* (para la CLI), introducir el valor "5".

54. Para que el periodo de inactividad surja efecto en la CLI, el *Login Shell* tiene que ser modificado al menos alguno de los siguientes tres ficheros:

```
/bin/csh
/bin/sh
/bin/tcsh
```

55. Esta acción debe ser realizada en la sección de *User Information* de la Web GUI, para cada usuario. Si el *Login Shell* se mantiene a su valor por defecto, el periodo de inactividad no será aplicado a la interfaz CLI.

56. Para limitar el acceso a la funcionalidad de *configd*, se debe realizar la siguiente configuración:

    - Crear un nuevo directorio que almacenará la nueva configuración, permitiendo interaccionar solamente con la funcionalidad de configd a los usuarios permitidos:

```
mkdir /usr/local/opnsense/service/conf/configd.conf.d
```

    - Copiar las siguientes líneas de código en un archivo denominado "*lockdown.conf*" y almacenarlo en el directorio previamente creado:

```
[actions_defaults]
allowed_groups = wheel
```

    - Reiniciar el servicio *configd* con el fin de aplicar los cambios:

```
service configd restart
```

57. Por defecto, cualquier usuario tiene permisos de lectura del archivo que contiene las credenciales y las claves privadas que emplea el TOE. Para limitar el acceso al archivo, de modo que solo los administradores puedan tener acceso, es necesario ejecutar con el usuario *root* el comando ***chmod 640 /conf/config.xml*** a través de la CLI.

6.3 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

58. La configuración de los interfaces de red en capa 2 y 3 OSI se realiza de forma segura durante la configuración inicial del sistema en la instalación, sin necesidad de tener conectado físicamente el equipo a ninguna red. Pueden consultarse los detalles en la dirección *https://docs.opnsense.org/manual/install.html#initial-configuration* [REF11].

59. El producto se puede gestionar local o remotamente según se indica en el Apartado *ADMINISTRACIÓN LOCAL Y REMOTA*. Se recomienda asignar un interfaz donde presentar la web de gestión, y tras esto emplear un equipo securizado con cable directo a dicho interfaz para acceder a la web de administración, donde se tendrá acceso a todas las opciones de configuración del producto.

60. En la dirección https://docs.opnsense.org/interfaces.html [REF12] se recogen los distintos tipos de interfaces y parámetros que soporta el sistema. Se soportan Ipv4 e Ipv6, así como interfaces físicos y virtuales (*bridges, GIF, GRE, LAGG, loopback, VLAN, VXLAN*).

61. Los interfaces permiten asignarles un nombre descriptivo y una descripción, así como una MAC e IP, así como habilitarlos o deshabilitarlos.

62. Para cada interfaz, entre otras opciones, se puede especificar:

    - *Block private networks*, si se activa esta opción, bloqueará en ese interfaz todo el tráfico procedente de direcciones privadas indicadas en el RFC 1918.
    - *Block bogon networks*, si se activa esta opción, bloqueará en ese interfaz todo el tráfico procedente de direcciones reservadas (pero no recogidas en RFC 1918) o aún no asignadas por IANA.

6.4 GESTIÓN DE CERTIFICADOS

63. Por defecto, se emplean certificados auto firmados. Estos deben reemplazarse con un certificado personalizado, el cual puede configurarse a través del menú `System > Trust > Certificates`.

64. El certificado generado tiene que ser generado con RSA-3072 o superior.

6.5 SINCRONIZACIÓN

65. OPNsense dispone de un servidor NTP que puede configurarse para sincronizar con otros servidores de hora en Internet, así como servir como fuente de sincronización horaria si se necesita en las redes a las que se conecta. Pueden consultarse los detalles en la dirección: https://docs.opnsense.org/manual/ntpd.html?highlight=ntp [REF13].

66. Por defecto, el producto está configurado para emplear los servidores NTP de Opnsense: <X.opnsense.pool.ntp.org>

67. La siguiente tabla muestra algunas de las opciones que pueden ser configuradas:

INTERFACE(S)	Interfaces to bind to, when none is selected it listens to all
Time servers	*Servers to use, comes with two toggles:* • ***Prefer*** *Marks the server as preferred.* • ***Do not use*** *Marks the server as unused, except for display purposes. The server is discarded by the selection algorithm*
Orphan mode	Orphan mode allows the system clock to be used when no other clocks are available. The number here specifies the stratum reported during orphan mode and should normally be set to a number high enough to insure that any other servers available to clients are preferred over this server.
NTP graphs	Enable RRD graphs of NTP statistics, which can be viewed in Reporting ‣ Health
Syslog logging	Extend logging with peer and/or system messages
Statistics logging	Enable statistical logging in /var/log/ntp, doesn't come with a user interface
Access restrictions	Within the access restriction row, you can set various options which limit the use of ntpd and in some cases instruct ntpd how to handle rejected clients.
Leap seconds	You can manually supply ntpd with a leap seconds file, more detailed info on the contents of those files can be found here.

Tabla 1. Opciones de configuración de NTP

6.6 ACTUALIZACIONES

68. **Se debe mantener el producto actualizado, sobre todo en lo que respecta a parches de seguridad**. Las actualizaciones del producto se realizarán mediante el menú `System → Firmware → Updates`.

69. El sistema conectará con los servidores pertinentes en Internet y comprobará si existen actualizaciones, tanto del sistema como de *plugins* instalados, bases de datos de filtrado, antivirus, *antispam*, etc.., ofreciendo mediante el interfaz web indicaciones relativas a las actualizaciones, tales como las versiones nuevas y si el sistema requiere un reinicio tras

actualizar. Es posible consultar más detalles en la dirección: https://docs.opnsense.org/manual/firmware.html#updates [REF14]

70. Se puede configurar la instalación automática de actualizaciones mediante el menú `System → Settings → Cron`, agregando un Job mediante el botón *ADD*, y seleccionando el valor *Automatic firmware update* en el campo *Command*, tal y como se muestra en las siguientes capturas de pantalla.

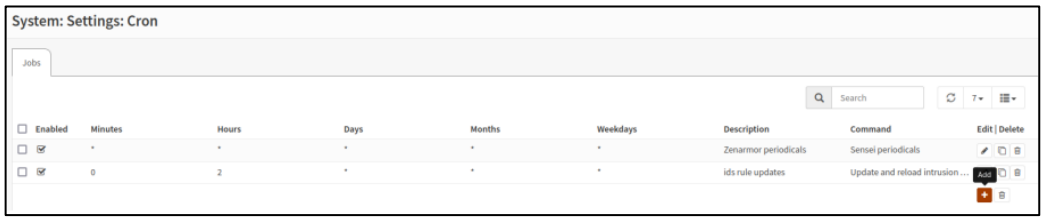

Ilustración 1. Interfaz gráfica de Cron tab

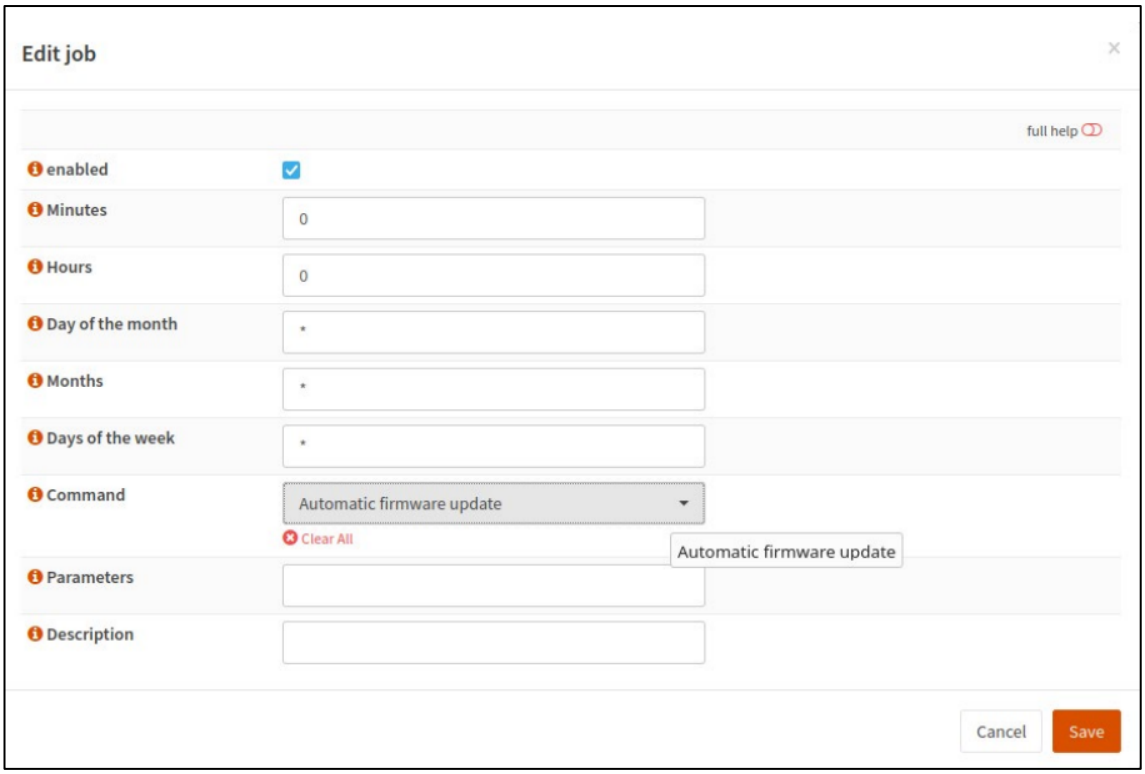

Ilustración 2. Activando las actualizaciones automáticas

71. Para más información acerca del proceso de instalación de actualización, se recomienda consultar el siguiente enlace: https://docs.opnsense.org/manual/updates.html [REF14]

6.7 AUDITORÍA

6.7.1 REGISTRO DE EVENTOS

72. Para habilitar el registro de eventos relacionados con todos los accesos, es necesario habilitar el parámetro "*enable access log*" en el menú `System > Settings > Administration`.

73. Para registrar los paquetes gestionados por una regla de cortafuegos, es necesario habilitar la opción de "*Log*" en el menú `Firewall > Rules > LAN` para cada regla que se considere relevante.

74. Para tener un registro preciso de los cambios en la configuración, incluyendo información adicional a la que contienen los registros de auditoría, se tiene que navegar hasta `System > Configuration > History` en la interfaz gráfica de usuario.

75. Por defecto, todos los registros de auditoría no son enviados al servidor Syslog. Por tanto, se debe realizar la siguiente configuración:

76. Editar el archivo /usr/local/opnsense/service/templates/OPNsense/Syslog/syslog-ng-destinations.conf añadiendo la siguiente línea:

```
{% set prog_list = prog_list + ['program("sshd")'] %}
```

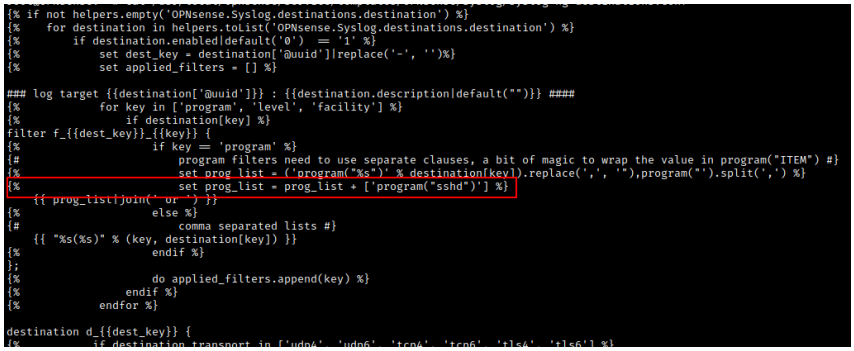

Ilustración 3. Editado del fichero syslog

77. Para que los cambios tengan efecto, habrá que guardar el archivo y reiniciar el servicio *syslog-ng*.

78. Por defecto, los usuarios tienen permiso para ver los registros de auditoría, con la contraparte de que también pueden eliminarlos. Con el fin de prevenir que los usuarios (excepto el usuario *root*) puedan eliminar los registros de auditoría, se debe aplicar la siguiente configuración:

    - Crear un nuevo directorio que almacene el nuevo ACL, ejecutando del siguiente comando:

```
mkdir -p /usr/local/opnsense/mvc/app/models/security/security/ACL
```

    - Copiar las siguientes líneas de código en un archivo XML llamado "ACL.xml" y almacenarlo en el directorio previamente creado:

```
<acl>
<page-diagnostics-logs-read-only>
<name>read only logs</name>
<patterns>
<!--  System: Log Files: Backend  -->
<pattern>ui/diagnostics/log/core/configd</pattern>
<pattern>api/diagnostics/log/core/configd</pattern>
<pattern>api/diagnostics/log/core/configd/export*</pattern>
<!--  System: Log Files: Audit  -->
<pattern>ui/diagnostics/log/core/audit</pattern>
<pattern>api/diagnostics/log/core/audit</pattern>
<pattern>api/diagnostics/log/core/audit/export*</pattern>
<!--  System: Log Files: Boot  -->
```

```
<pattern>ui/diagnostics/log/core/boot</pattern>
<pattern>api/diagnostics/log/core/boot</pattern>
<pattern>api/diagnostics/log/core/boot/export*</pattern>
<!--  System: Log Files: General  -->
<pattern>ui/diagnostics/log/core/system</pattern>
<pattern>api/diagnostics/log/core/system</pattern>
<pattern>api/diagnostics/log/core/system/export*</pattern>
<!--  System: Log Files: Web GUI  -->
<pattern>ui/diagnostics/log/core/lighttpd</pattern>
<pattern>api/diagnostics/log/core/lighttpd</pattern>
<pattern>api/diagnostics/log/core/lighttpd/export*</pattern>
<!--  Firewall: Log Files: General  -->
<pattern>ui/diagnostics/log/core/firewall</pattern>
<pattern>api/diagnostics/log/core/firewall</pattern>
<pattern>api/diagnostics/log/core/firewall/export*</pattern>
<!--  Firewall: Log Files: Live View  -->
<pattern>ui/diagnostics/firewall/log</pattern>
<pattern>api/diagnostics/firewall/log/*</pattern>
<!--  Firewall: Log Files: Overview  -->
<pattern>ui/diagnostics/firewall/stats</pattern>
<pattern>api/diagnostics/firewall/stats*</pattern>
<!--  Firewall: Log Files: Plain View  -->
<pattern>ui/diagnostics/log/core/filter</pattern>
<pattern>api/diagnostics/log/core/filter</pattern>
<pattern>api/diagnostics/log/core/filter/export*    /pattern>
</patterns>
</page-diagnostics-logs-read-only>
</acl>
```

- Limpiar la caché, para prevenir que el ACL anterior siga en uso, con el siguiente comando:

```
rm /tmp/opnsense_acl_cache.json
```

79. Con la configuración anterior, se habilita un nuevo permiso llamado “read only logs”. Este permiso se le puede asignar a los usuarios a los que se desee que puedan leer los registros de auditoría.

80. El sistema genera y almacena los siguientes eventos, en ficheros en formato de texto plano:

TIPO DE EVENTO	ACCESIBLE EN…	DESCRIPCIÓN
System Log	*System → Log Files → General*	Eventos del propio sistema
Audit	*System → Log Files → Audit*	Acciones de los usuarios
Backend/config daemon	*System → Log Files → Backend*	Eventos de generación de configuraciones por el uso de la API
Web GUI	*System → Log Files → Web GUI*	Eventos del propio servidor web que publica la interfaz web de administración (Lighttpd)
Firmware	*System → Firmware → Log File*	Eventos de actualizaciones del sistema

Gateways	*System → Gateways → Log File*	Eventos relativos al seguimiento de puertas de enlace de Dpinger
Routing	*System → Routes → Log File*	Eventos de interfaces o cambios de rutas

Tabla 2. Eventos Generados

81. Todos los tipos de eventos pueden filtrarse por *Severity (Emergency, Alert, Critical, Error, Warning, Notice, Informational y Debug)* y buscarse mediante cadena de caracteres en el campo *Search*.

6.7.2 ALMACENAMIENTO LOCAL

82. El sistema almacena internamente los registros de los eventos de forma predeterminada, en la carpeta del sistema /var/log.

83. En caso de alcanzar el límite del almacenamiento interno, el sistema sobrescribirá los registros más antiguos.

6.7.3 ALMACENAMIENTO REMOTO

84. Es posible configurar el almacenamiento en un sistema externo, configurando syslog-ng para enviar la información de auditoría mediante `System → Settings → Logging/targets`, y agregando un servidor Syslog remoto.

85. Los parámetros para definir el servidor remoto Syslog son los siguientes:

    - *Transport* = Protocolo de transporte a emplear en el envío de los registros de eventos, debe ser TLS (4), sobre IPv4, o TLS (6) sobre IPv6. Es factible no seleccionar TLS, pero en ese caso la comunicación hacia el servidor remoto deberá realizarse mediante una VPN (IPsec, OpenVPN, etc.) por motivos de seguridad.
    - *Applications* = Conjunto de aplicaciones de las que se desea enviar los registros de eventos al servidor Syslog remoto. Si no se indica nada se consideran todas.
    - *Levels* = Niveles de Syslog, tal y como se recogen en el RFC5424, que se desea enviar. Si no se indica nada se consideran todos.
    - *Facilities* = Conjunto de *facilities* a enviar. Si no se indica nada se consideran todas.
    - *Hostname* = Servidor Syslog remoto.
    - Port = Puerto del servidor remoto al que enviar los registros.
    - *Certificate* = Certificado digital, instalado en el sistema a usar para el cifrado del tráfico a enviar.
    - RFC5424 = Marcar para indicar si los mensajes a remitir al servidor remoto siguen el formato indicado en dicha RFC

86. Para más información al respecto, se recomienda consultar el siguiente enlace: https://docs.opnsense.org/manual/settingsmenu.html [REF15].

6.8 BACKUP

87. Para realizar copias de seguridad, es necesario ir a la ruta `System > Configuration > Backup` y establecer un valor de 5 o superior en el campo de *Backup Count*.

88. De esta forma cada vez que se realice un cambio en la configuración o cada vez que se creen, modifiquen o eliminen reglas de *firewall*, se genera una copia de seguridad.

89. Se almacenan las últimas 5 configuraciones, estableciendo una política de rotación siguiendo el criterio de eliminar el más antiguo.

6.9 AUTO-CHEQUEOS

El sistema permite realizar auto-chequeos bajo demanda, a través del menú `System > Firmware > Status`, pulsando el botón "*Run an audit*" es posible seleccionar los distintos auto-chequeos:

- Connectivity: comprueba la conectividad con los distintos repositorios que ofrecen el software y paquetes que usa el sistema.
- Health: revisa si el kernel instalado es correcto, buscando ficheros perdidos o alterados, así como del software de base, repositorios y plugins y paquetes de software instalados. Revisa también si existen dependencias incumplidas.
- Security: comprueba los paquetes de software que presenten algún tipo de vulnerabilidad, ofreciendo el CVE pertinente del mismo e información al respecto.
- Upgrade: muestra un reporte completo de las actualizaciones realizadas en el sistema.

90. Para cada tipo de chequeo se muestra la salida de consola del sistema, mostrando la información pertinente en caso de errores como ayuda para la solución de los mismos.

91. Para más información al respecto, se recomienda consultar el enlace: https://docs.opnsense.org/security.html [REF16]

6.10 ALTA DISPONIBILIDAD

92. El software permite la configuración de alta disponibilidad utilizando el protocolo libre *Common Address Redundancy Protocol (CARP)* [REF23] para configurar conjuntos de dos o más sistemas en alta disponibilidad activo-pasivo, permitiendo la sincronización de las conexiones de red establecidas y las políticas y configuraciones aplicadas entre ellos.

93. En caso de querer habilitarlo, se deben configurar direcciones IP virtuales en todos los interfaces. En caso de error del sistema activo, el sistema pasivo con mayor prioridad adquirirá dichas IP virtuales en sus propios interfaces y continuará prestando el servicio, manteniendo las conexiones previamente abiertas sin interrupción de la comunicación.

94. La configuración se realiza a través del menú *System* → *High Availability* → *Settings*.

95. Los detalles de la configuración y opciones recomendadas pueden consultarse en la dirección https://docs.opnsense.org/manual/hacarp.html [REF22].

96. Asimismo, se recomienda consultar el siguiente enlace: https://docs.opnsense.org/manual/how-tos/carp.html [REF23].

6.11 SERVICIOS DE SEGURIDAD

97. A través de `System → Firewall`, es posible gestionar las **políticas de cortafuegos** con inspección de estados (*Stateful firewall*). Para obtener información detallada sobre la

funcionalidad completa del firewall, se recomienda consultar el siguiente enlace: https://docs.opnsense.org/firewall.html [REF17].

98. OPNsense soporta *TCP*, *UDP*, *ESP* y *AH* sobre *Ipv4* e *IPv6*, pudiendo especificar reglas de filtrado de paquetes sobre dichos protocolos, tanto en dirección de entrada a cualquier interfaz o conjunto de ellos (por defecto), como en dirección de salida de los mismos.

99. Mediante `System → Firewall → Aliases` el sistema permite definir nombres descriptivos para *hosts*, *redes*, *puertos*, *URL*, *direcciones MAC*, *BGP ASN* y algunos tipos más avanzados. El uso de alias permite simplificar, agrupar y facilitar la comprensión de las reglas de filtrado del cortafuegos. Esta información se puede consultar en el siguiente enlace: https://docs.opnsense.org/manual/aliases.html [REF18].

100. Es posible definir Categorías (*category*) con un nombre y un color, como un elemento identificador para diferenciar distintos tipos de reglas, pudiendo gestionarlas a través de `System → Firewall → Categories`.

101. Mediante `System → Firewall → Groups`, es posible agrupar varios interfaces de red bajo un nombre común, con objeto de poder aplicar reglas de filtrado sobre conjuntos de interfaces.

102. A través del menú `System → Firewall → NAT`, se dispone de diversas opciones de traducción de direcciones IP y puertos TCP/UDP, incluido NPT. Para obtener información detallada al respecto, se recomienda consultar el siguiente enlace: https://docs.opnsense.org/manual/nat.html [REF19]

103. Las reglas de filtrado se gestionan a través de `System → Firewall → Rules`. El sistema presenta un submenú con todos los interfaces (físicos, virtuales, de VPN o agrupados) existentes, además de otro denominado "*Floating*". Éste último submenú sirve como sitio donde agregar reglas que se aplicarán a todos los interfaces, y con mayor prioridad que las reglas asociadas a éstos, tal y como se indica a continuación. Las reglas de filtrado de un paquete de datos que intenta atravesar un interfaz del sistema se comprobarán en el siguiente orden:

    - Interfaz *Floating*.
    - Grupos de interfaces a los que pertenezca el interfaz al que llega el paquete.
    - Interfaz al que llega el paquete.

104. OPNsense recorrerá la lista de reglas de dichos interfaces de arriba a abajo, si encuentra una regla que coincide con el paquete con el parámetro "*quick*" activo (por defecto), la aplicará y no seguirá inspeccionando el resto de reglas. En el caso de que se haya desactivado la opción "*quick*", el sistema seguirá comprobando reglas hasta encontrar alguna que coincida con el paquete a procesar. Si todas las reglas aplicables tienen la opción "*quick*" desactivada, se aplicará la última de ellas. En caso de no encontrar ninguna regla, se aplicarán las reglas por defecto existentes.

105. Los parámetros más importantes de una regla son:

PARÁMETROS PRINCIPALES DE UNA REGLA DE CORTAFUEGOS	
Action	Acción a efectuar con el paquete si aplica esta regla: *Pass* = Se permite al paquete continuar.

	Reject = Se impide al paquete continuar y se remite al origen del mismo un paquete indicándolo. *Block* = Se impide al paquete continuar.
Disabled	Si la regla está desactivada. Por defecto desmarcado.
Quick	Si la regla se aplica inmediatamente. Por defecto marcado.
Interface	Interfaz o interfaces donde se aplica la regla.
Direction	Dirección del tráfico: - *in* = entrando al interfaz (por defecto). - *out* = saliendo del interfaz. - *any* = entrando y saliendo del interfaz.
TCP/IP Version	Versión del protocolo IP en la que aplica: IPv4, IPv6 o IPv4+IPv6.
Protocol	Protocolo IP en el que aplica: any, TCP, UDP, TCP/UDP o ICMP.
Source	Origen del tráfico.
Destination	Destino del tráfico.
Destination port range	Puerto o rango de puertos en el destino donde se dirige el tráfico.
Log	Si queremos que la regla emita un registro de evento cuando aplique a tráfico.
Category	Categoría a la que pertenece la regla.
Description	Texto descriptivo.

Tabla 3. Parámetros principales de una regla de cortafuegos

106. Un ejemplo de una regla para permitir el tráfico entre un dispositivo origen denominado "*EquipoOrigen*" hacia un dispositivo destino denominado "*EquipoDestino*" al puerto TCP 1433 y registrando el tráfico asociado:

EJEMPLO REGLA PERMITIR TRÁFICO	
Action	Pass
Disabled	Desmarcar
Quick	Marcar
Interface	LAN
Direction	in
TCP/IP Version	IPv4
Protocol	TCP
Source	EquipoOrigen
Destination	EquipoDestino
Destination port range - from	1433

Destination port range - to	1433
Log	Marcar

Tabla 4. Ejemplo regla de cortafuegos

107. OPNsense dispone de diversas **opciones** en las reglas para evitar ataques (Dos, Botnets, etc.). Dichas opciones son accesibles en la sección "*Advanced Options*" de una regla, pulsando el botón "*Show/Hide*". Las opciones existentes son:

- *Max states* = Número máximo de entradas en la tabla de estados de las conexiones que puede crear.
- *Max source nodes* = Número máximo de equipos origen únicos del tráfico.
- *Max established* = Número máximo de conexiones TCP establecidas por equipo origen.
- *Max source states* = Número máximo de entradas en la tabla de estados que puede crear un mismo equipo origen.
- *Max new connections* = Número máximo de conexiones por equipo origen o por segundo.
- *State timeout* = Tiempo de vida máximo en segundos de una conexión TCP.
- *Adaptative Timeouts* = Umbrales *start* y *end* para adaptar el tiempo de vida de las conexiones TCP según el crecimiento del número de conexiones establecidas.

108. Otra opción muy recomendable es usar bases de datos de IP en función de su situación geográfica, para aplicar reglas en función de países/continentes/regiones. En el menú `System → Firewall → Aliases` se deberá crear alias de tipo GeoIP. En la pestaña "*GeoIP settings*" es posible especificar el servidor al que el sistema consultará de manera automática para refrescar el listado de IP y zona geográfica asociada.

109. Es conveniente también, con objeto de seguir el principio de **mínimo privilegio**, hacer uso de *Schedules* (planificaciones) para asociar a las reglas. De esta manera, una regla con un Schedule asociado solo aplicará si el momento temporal en el que se comprueba entra dentro del período de tiempo establecido en dicho *Schedule*. Éstos se pueden gestionar desde el menú `System → Firewall → Settings → Schedules`. Para más información al respecto, se recomienda consultar el siguiente enlace: https://docs.opnsense.org/manual/firewall_settings.html#schedules [REF20].

110. Por último, OPNsense permite implementar normalización sobre los paquetes de datos que recibe, para evitar inconsistencias y posibles ataques. Para más información al respecto, se recomienda consultar el siguiente enlace:

https://docs.opnsense.org/manual/firewall_scrub.html [REF21].

7 REFERENCIAS

[REF1] OPNsense – CARP
https://docs.opnsense.org/manual/how-tos/carp.html

[REF2] Suricata
https://suricata.io/

[REF3] Netmap
https://manpages.ubuntu.com/manpages/bionic/man4/netmap.4freebsd.html

[REF4] Página de descarga de OPNsense
https://opnsense.org/download

[REF5] OPNsense Instalación inicial y configuración
https://docs.opnsense.org/manual/install.html

[REF6] OPNsense Legal Notices
https://docs.opnsense.org/legal.html

[REF7] OPNsense Hardware Sizing and Setup
https://docs.opnsense.org/manual/hardware.html

[REF8] OPNsense Virtual and Cloud-based Installation
https://docs.opnsense.org/manual/virtuals.html

[REF9] OPNsense Two-Factor Authentication
https://docs.opnsense.org/manual/two_factor.htm

[REF10] OPNsense User Management - Users and Groups
https://docs.opnsense.org/manual/how-tos/user-local.html

[REF11] OPNsense Initial Configuration
https://docs.opnsense.org/manual/install.html#initial-configuration

[REF12] OPNsense Interfaces
https://docs.opnsense.org/interfaces.html

[REF13] OPNsense - Network Time
https://docs.opnsense.org/manual/ntpd.html?highlight=ntp

[REF14] OPNsense – Updates
https://docs.opnsense.org/manual/firmware.html#updates

[REF15] OPNsense - System Settings
https://docs.opnsense.org/manual/settingsmenu.htm

[REF16] OPNsense – Security
https://docs.opnsense.org/security.html

[REF17] OPNsense – Firewall
https://docs.opnsense.org/firewall.html

[REF18] OPNsense – Aliases
https://docs.opnsense.org/manual/aliases.html

[REF19] OPNsense – NAT
https://docs.opnsense.org/manual/nat.html

[REF20] OPNsense – Schedules
https://docs.opnsense.org/manual/firewall_settings.html#schedules

[REF21] OPNsense - Firewall Normalization
https://docs.opnsense.org/manual/firewall_scrub.html

[REF22] OPNsense - High Availability
https://docs.opnsense.org/manual/hacarp.html

[REF23] OPNsense – CARP
https://docs.opnsense.org/manual/how-tos/carp.html

8 ABREVIATURAS

ACL	Access Control List
AES	Advanced Encryption Standard
AMD64	Advanced Micro Devices 64-bit Architecture
API	Application Programming Interface
BGP ASN	Border Gateway Protocol Autonomous System Number
BSD	Berkeley Software Distribution
CARP	Common Address Redundancy Protocol
CLI	Command Line Interface
CPSTIC	Catálogo de productos STIC
CPU	Central Processing Unit
CVE	Common Vulnerabilities and Exposures
DoS	Denial of Service
DVD	Digital Versatile Disc
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ENS	Esquema Nacional de Seguridad
GCM	Galois/Counter Mode
GIF	Generic Interface
GRE	Generic Routing Encapsulation
GUI	Graphical User Interface
HTTPS	HyperText Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IPSEC	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISO	International Organization for Standardization
LAGG	Link Aggregation
LAN	Local Area Network
MAC	Message Authentication Code
NAT	Network Address Translation
NPT	Network Prefix Translation
NTP	Network Time Protocol

OpenSSL	Open Secure Sockets Layer
OpenVPN	Open Source Virtual Private Network
RAM	Random Access Memory
RFC	Request for Comments
RRD	Round Robin Database
SSH	Secure Shell
SSHv2	Secure Shell version 2
SSL	Secure Sockets Layer
STIC	Seguridad de las Tecnologías de la Información y las Comunicaciones
Syslog	System Logging Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TOTP	Time-based One-Time Password
UDP	User Datagram Protocol
UEFI	Unified Extensible Firmware Interface
URL	Uniform Resource Locator
USB	Universal Serial Bus
VGA	Video Graphics Array
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VXLAN	Virtual Extensible LAN
WAN	Wide Area Network
XML	Extensible Markup Language


PUBLICACIONES
Pd
DE DEFENSA


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