





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

Edita:



Pº de la Castellana 109, 28046 Madrid  
© Centro Criptológico Nacional, 2023

NIPO: 083-23-284-X.

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**

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

## ÍNDICE

<b>1. INTRODUCCIÓN</b> .....	<b>4</b>
<b>2. OBJETO Y ALCANCE</b> .....	<b>5</b>
<b>3. ORGANIZACIÓN DEL DOCUMENTO</b> .....	<b>6</b>
<b>4. FASE PREVIA A LA INSTALACIÓN</b> .....	<b>7</b>
4.1 ENTREGA SEGURA DEL PRODUCTO .....	7
4.2 ENTORNO DE INSTALACIÓN SEGURO .....	8
4.3 REGISTRO Y LICENCIAS .....	8
4.4 CONSIDERACIONES PREVIAS .....	8
<b>5. FASE DE INSTALACIÓN</b> .....	<b>9</b>
<b>6. FASE DE CONFIGURACIÓN</b> .....	<b>10</b>
6.1 MODO DE OPERACIÓN SEGURO .....	10
6.2 AUTENTICACIÓN.....	13
6.3 ADMINISTRACIÓN DEL PRODUCTO.....	14
6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA.....	14
6.3.2 CONFIGURACIÓN DE ADMINISTRADORES .....	16
6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS.....	18
6.5 GESTIÓN DE CERTIFICADOS.....	18
6.6 SERVIDORES DE AUTENTICACIÓN .....	21
6.7 SINCRONIZACIÓN .....	22
6.8 ACTUALIZACIONES .....	23
6.9 AUTO-CHEQUEOS.....	24
6.10 ALTA DISPONIBILIDAD.....	25
6.11 AUDITORÍA .....	26
6.11.1 REGISTRO DE EVENTOS .....	26
6.12 ALMACENAMIENTO LOCAL .....	27
6.12.1 ALMACENAMIENTO REMOTO .....	27
6.13 BACKUP .....	28
6.14 SERVICIOS DE SEGURIDAD .....	29
<b>7. FASE DE OPERACIÓN</b> .....	<b>33</b>
<b>8. CHECKLIST</b> .....	<b>34</b>
<b>9. REFERENCIAS</b> .....	<b>38</b>
<b>10. ABREVIATURAS</b> .....	<b>41</b>

## 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* [REF28], permitiendo un clúster en modo activo/pasivo.
  - Detección y Prevención de Intrusión (*Intrusion Detection & Prevention*) usando *Suricata* [REF9] y *Netmap* [REF10], 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*.

## 2. OBJETO Y ALCANCE

9. El objeto del presente documento es servir como guía para realizar una instalación, configuración y operación segura del cortafuegos *software* **OPNsense versión 21.7** (versión gratuita), y **OPNsense Business Edition 22 y 23** (versión comercial).
10. **Dichos productos han sido cualificados e incluidos en el Catálogo de Productos y Servicios STIC (CPSTIC) del Centro Criptológico Nacional.** Se recomienda consultar la versión cualificada en cada momento.

### 3. ORGANIZACIÓN DEL DOCUMENTO

11. El documento se divide en los siguientes apartados:

- **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** – En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.
- **Apartado 8**– En este apartado se muestra una lista de tareas a revisar para verificar que se han llevado a cabo cada una de las recomendaciones y configuraciones descritas en la presente guía de empleo seguro.
- **Apartado 9**- Este apartado contiene la documentación a la que se ha hecho referencia a lo largo de este documento.
- **Apartado 10**- Este apartado contiene las abreviaturas que han sido empleadas 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/> [REF11]. La descarga y verificación de la misma se realizarán conforme a lo indicado en <https://docs.opnsense.org/manual/install.html> [REF12], 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 .bz2 (<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](#) [REF11].
  - 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*.

## 4.3 REGISTRO Y LICENCIAS

24. Siendo *software* libre, se descarga desde la dirección <https://opnsense.org/download/> [REF11] sin necesidad de registro.
25. El licenciamiento puede consultarse en la dirección <https://opnsense.org/about/legal-notices/> [REF13], siendo una licencia de tipo BSD 2-Clause simplificada.

## 4.4 CONSIDERACIONES PREVIAS

26. 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> [REF14].
27. 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.
28. 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> [REF15].

## 5. FASE DE INSTALACIÓN

29. 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> [REF12].
30. 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.
31. 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.
32. Una vez descargada y verificada la imagen de instalación, se procederá a escribir dicha imagen en un disco USB o IDE, tal y como se indica en el siguiente enlace: <https://docs.opnsense.org/manual/install.html#installation-method> [REF16].
33. Se iniciará el dispositivo, configurado previamente para que arranque del USB o IDE donde se ha escrito la imagen de instalación. El sistema arrancará, ofreciendo diversas opciones de configuración. Dichas opciones de configuración se detallan en <https://docs.opnsense.org/manual/install.html#initial-configuration> [REF17]. Una vez iniciado el sistema, se iniciará un entorno de ejecución “live” arrancado desde el USB o IDE, sin modificar nada del almacenamiento interno del dispositivo.
34. Una vez terminada la configuración, habrá que reiniciar el dispositivo para que arranque desde su almacenamiento local, en lugar del USB o IDE de instalación.
35. El sistema arrancará, y ofrecerá un interfaz web de administración sobre aquellos interfaces escogidos en la configuración inicial.
36. Existen guías de instalación para entornos alternativos, tales como aquellos con acceso por puerto serie, o sobre instancias AWS o Azure. Estas guías pueden ser consultadas en <https://docs.opnsense.org/setup.html#setup-guides> [REF18].
37. 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> [REF14]
38. 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> [REF15]

## 6. FASE DE CONFIGURACIÓN

### 6.1 MODO DE OPERACIÓN SEGURO

#### 39. Se deben seguir los siguientes pasos para reforzar la seguridad en el arranque del sistema:

- Acceder al *shell* de comandos, conectándose mediante SSHv2 y accediendo al menú de consola que aparece mediante la opción número 8), tal y como se muestra en la imagen siguiente:

```
ssh root@192.168.1.1
Password:
Last login: Fri Mar 31 19:53:26 2023 from 192.168.1.100
-----
Hello, this is OPNsense 22.7 | @@@@@@@@@@@@@@@@
Website: https://opnsense.org/ | @@@@ @@@@
Handbook: https://docs.opnsense.org/ | @@@@\\ //@@@
Forums: https://forum.opnsense.org/ | ))))))) ((((((
Code: https://github.com/opnsense | @@@// \\@@@
Twitter: https://twitter.com/opnsense | @@@@ @@@@
-----
*** OPNsense (amd64/LibreSSL) ***

DMZ (vtnet0) -> v4: 192.168.1.100/24
SYN (vtnet2) -> v4: 192.168.1.100/24
TERMOPILAS (vtnet1) -> v4: 192.168.1.100/24

HTTPS: SHA256 [REDACTED]
SSH: SHA256 [REDACTED]
SSH: SHA256 [REDACTED]
SSH: SHA256 [REDACTED]

0) Logout                7) Ping host
1) Assign interfaces     8) Shell
2) Set interface IP address 9) pfTop
3) Reset the root password 10) Firewall log
4) Reset to factory defaults 11) Reload all services
5) Power off system       12) Update from console
6) Reboot system         13) Restore a backup

Enter an option: 8
```

Figura 1 - "Selección de opción 8) Shell"

- Editar el fichero `/usr/local/etc/rc.bootup` y antes de la línea que contiene el texto `"interfaces_configure(true);"` agregar una línea con el contenido `"filter_configure_sync(true);"`, como se puede observar en la imagen siguiente.

```
system_kernel_configure(true);
system_sysctl_configure(true);
system_timezone_configure(true);
system_firmware_configure(true);
system_trust_configure(true);
system_hostname_configure(true);
system_hosts_generate(true);
system_syslog_start(true);
filter_configure_sync(true);
interfaces_configure(true);
system_resolvconf_generate(true);
filter_configure_sync(true);
plugins_configure('early', true);
system_routing_configure(true);
system_hosts_generate(true);
plugins_configure('dhcp', true);
plugins_configure('dhcrelay', true);
plugins_configure('dns', true);
plugins_configure('monitor', true);
filter_configure_sync(true);
plugins_configure('vpn', true);
plugins_configure('bootup', true);
rrd_configure(true);
system_kernel_configure(true);
system_sysctl_configure(true);
system_timezone_configure(true);
system_firmware_configure(true);
system_trust_configure(true);
system_hostname_configure(true);
system_hosts_generate(true);
system_syslog_start(true);
filter_configure_sync(true);
interfaces_configure(true);
system_resolvconf_generate(true);
filter_configure_sync(true);
plugins_configure('early', true);
system_routing_configure(true);
system_hosts_generate(true);
plugins_configure('dhcp', true);
plugins_configure('dhcrelay', true);
plugins_configure('dns', true);
plugins_configure('monitor', true);
filter_configure_sync(true);
plugins_configure('vpn', true);
plugins_configure('bootup', true);
rrd_configure(true);
```

Figura 2 - "Arranque seguro"

#### 40. Adicionalmente, deben realizarse las siguientes acciones:

- Sustituir OpenSSL en favor de LibreSSL, dado que éste último tiene un historial de seguridad mejor, desde el interfaz web de administración, accediendo a *System* → *Firmware* → *Settings* indicando el valor LibreSSL en el campo *Flavour*.
- El producto usa un certificado auto-firmado por defecto. Dicho certificado deberá ser sustituido por un certificado personalizado, con las características requeridas por la normativa de aplicación, a través de *System* → *Trust* → *Certificates*.
- La clave por defecto del administrador *root* deberá ser modificada en *System* → *Users*. Dicha clave debería tener una longitud mínima de 12 caracteres y estar compuesta de letras mayúsculas, minúsculas, números y caracteres especiales. La política de contraseñas puede modificarse en *System* → *Access* → *Servers*.
- Es necesario activar el parámetro *Enable access log* en *System* → *Settings* → *Administration*, en la sección Web GUI. Esto habilita el almacenamiento de todos los eventos correspondientes a accesos al interfaz web de administración en los archivos de auditoría, para depuración y/o análisis.
- Es necesario crear dos reglas de cortafuegos para evitar ataque DoS (*Denial of Service*), en la sección *Firewall* → *Rules*.
  - a. Permitir un máximo de 100 conexiones al interfaz de gestión web desde cualquier red distinta de la red de administración.
  - b. Permitir un máximo de 100 conexiones al interfaz de gestión web desde la red de administración, opcionalmente permitiendo sólo la dirección IP del administrador si ésta no fuera dinámica. **Esta segunda regla debe tener mayor prioridad que la anterior.**
- Para evitar ataques de degradación TLS al comunicar con un servidor Syslog externo, se debe acceder al sistema mediante consola o SSHv2 con permisos de administrador y modificar el fichero:
 

```
/usr/local/opnsense/service/templates/OPNsense/syslog/syslog-ng-destinations-conf,
```

 agregando el código `ssl-options(no-sslv2, no-sslv3, no-tls1, notls11)` y reiniciando el sistema para que los cambios surtan efecto, como se puede observar en la imagen siguiente.

```
ssl-options(no-sslv2, no-sslv3, no-tls1, notls11)
```

Figura 3 - Opciones SSL syslog-ng

41. Con objeto de cumplir los requisitos criptográficos indicados en la guía *CCN-STIC-807 Criptología de empleo en el Esquema Nacional de Seguridad*, se deben configurar las suites de cifrado aceptadas y los parámetros de las mismas:
- Suites de cifrado de TLS aceptadas para la interfaz web de administración, mediante *System* → *Settings* → *Administration*, sección Web GUI, parámetro SSL Ciphers, seleccionar el conjunto siguiente:

CONJUNTO DE VALORES PARA SSL CIPHER
TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384

CONJUNTO DE VALORES PARA SSL CIPHER
TLS_CHACHA20_POLY1305_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256

**Tabla 1 – Conjunto de valores para SSL Cipher**

- SSH mediante *System* → *Settings* → *Administration*, sección *Secure Shell*, seleccionar los conjuntos de valores indicados para los siguientes parámetros:

CONJUNTO DE VALORES PARA KEY EXCHANGE ALGORITHMS
diffie-hellman-group14-sha256
diffie-hellman-group16-sha512
diffie-hellman-group18-sha512
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521

**Tabla 2 – Conjunto de valores para Key Exchange algorithms**

CONJUNTO DE VALORES PARA CIPHERS
<i>aes128-gcm@openssh.com</i>
<i>aes256-gcm@openssh.com</i>

**Tabla 3 – Conjunto de valores para Ciphers**

CONJUNTO DE VALORES PARA MACS
<i>hmac-sha2-256</i>
<i>hmac-sha2-512</i>

**Tabla 4 – Conjunto de valores para MACs**

CONJUNTO DE VALORES PARA PUBLIC KEY SIGNATURE ALGORITHMS
<i>ecdsa-sha2-nistp256</i>
<i>ecdsa-sha2-nistp385</i>
<i>ecdsa-sha2-nistp521</i>

**Tabla 5 – Conjunto de valores para Public key signature algorithms**

42. Seleccionar el protocolo TLS para comunicaciones con servidor Syslog externo, a través del acceso por consola o mediante SSH, seleccionando la opción 8) Shell, tal y como se muestra en la siguiente captura de pantalla:

```

0) Logout
1) Assign interfaces
2) Set interface IP address
3) Reset the root password
4) Reset to factory defaults
5) Power off system
6) Reboot system
7) Ping host
8) Shell
9) pfTop
10) Firewall log
11) Reload all services
12) Update from console
13) Restore a backup
Enter an option: 8

```

Figura 4 - Accediendo a la Shell del producto

43. A continuación, habrá que agregar en la sección “network” del fichero `/etc/local/opnsense/service/templates/OPNsense/Syslog/syslog-ng-destinations.conf` las siguientes líneas:

```

ssl-options(no-sslv2, no-sslv3, no-tlsv1, no-tlsv11)

cipher-suite("ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-
SHA256:TLS_AES_128_GCM_SHA256:TLS_AES_128_GCM_SHA256:TLS_CHACHA20_POLY
1305_SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-
SHA384:ECDHE-ECDSA-AES256-CCM:ECDHE-ECDSA-AES128-CCM")

```

44. Se muestra una captura de pantalla como guía:

```

network(
  "{{destination.hostname}}"
  transport("tls")
  port({{destination.port}})
  ip-protocol({{destination.transport[3]}})
  persist-name("{{dest_key}}")
  tls(
    ca-file("/etc/ssl/cert.pem")
    key-file("/usr/local/etc/syslog-ng/cert.d/{{dest_key}}.key")
    cert-file("/usr/local/etc/syslog-ng/cert.d/{{dest_key}}.crt")
    ssl-options(no-sslv2, no-sslv3, no-tlsv1, no-tlsv11)
    cipher-suite("ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:TLS_AES_128_GCM-
SHA256:TLS_AES_128_GCM_SHA256:TLS_CHACHA20_POLY1305_SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-A-
ES256-GCM-SHA384:ECDHE-ECDSA-AES256-CCM:ECDHE-ECDSA-AES128-CCM")
  )
);

```

Figura 5 - Syslog-ng-destinations.conf

## 6.2 AUTENTICACIÓN

45. Los mecanismos de autenticación que utiliza son:

- Autenticación de usuarios, mediante credenciales locales (almacenadas en una base de datos interna), servidor externo LDAP, servidor externo RADIUS.
- Autenticación de servicios VPN, proxy web y portal cautivo mediante credenciales locales, servidor externo LDAP, servidor externo RADIUS, certificados digitales.
- Autenticación entre componentes del producto y/o con servidores o dispositivos externos, mediante certificados digitales.
- Autenticación de acceso SSH y acceso por consola mediante credenciales locales, servidor externo LDAP, servidor externo RADIUS.

46. A excepción del acceso por consola y por SSHv2, el sistema soporta autenticación de doble factor, tanto para acceder a la interfaz gráfica (GUI) de gestión como al portal cautivo, servicios VPN (IPSec y OpenVPN) y proxy caché. **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](https://docs.opnsense.org/manual/two_factor.html) [REF19].

47. Se debe minimizar el uso de claves precompartidas en los servicios donde sea posible, en favor del uso de certificados digitales y 2FA (*Two-Factor Authentication*), con objeto de maximizar la seguridad.
48. Para más información relativa a los mecanismos de autenticación del producto, se recomienda consultar el siguiente enlace:

<https://docs.opnsense.org/manual/users.html#authentication> [REF20]

## 6.3 ADMINISTRACIÓN DEL PRODUCTO

### 6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

49. El producto se administra localmente mediante acceso por consola, y remotamente tanto por un portal de administración web como por SSH.
50. Es posible reforzar la seguridad en el acceso a la gestión del sistema seleccionando *System* → *Settings* → *Administration* y definiendo las siguientes opciones, tal y como se observa en la imagen siguiente:

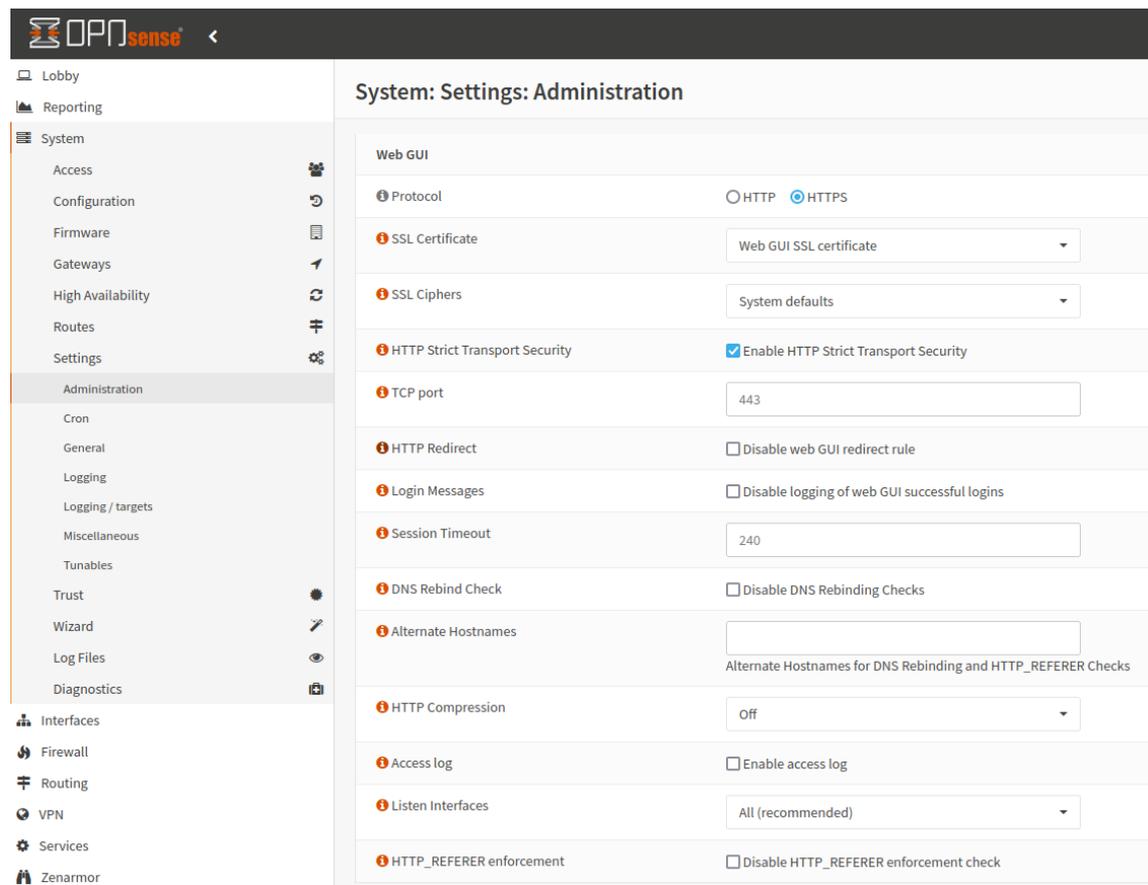
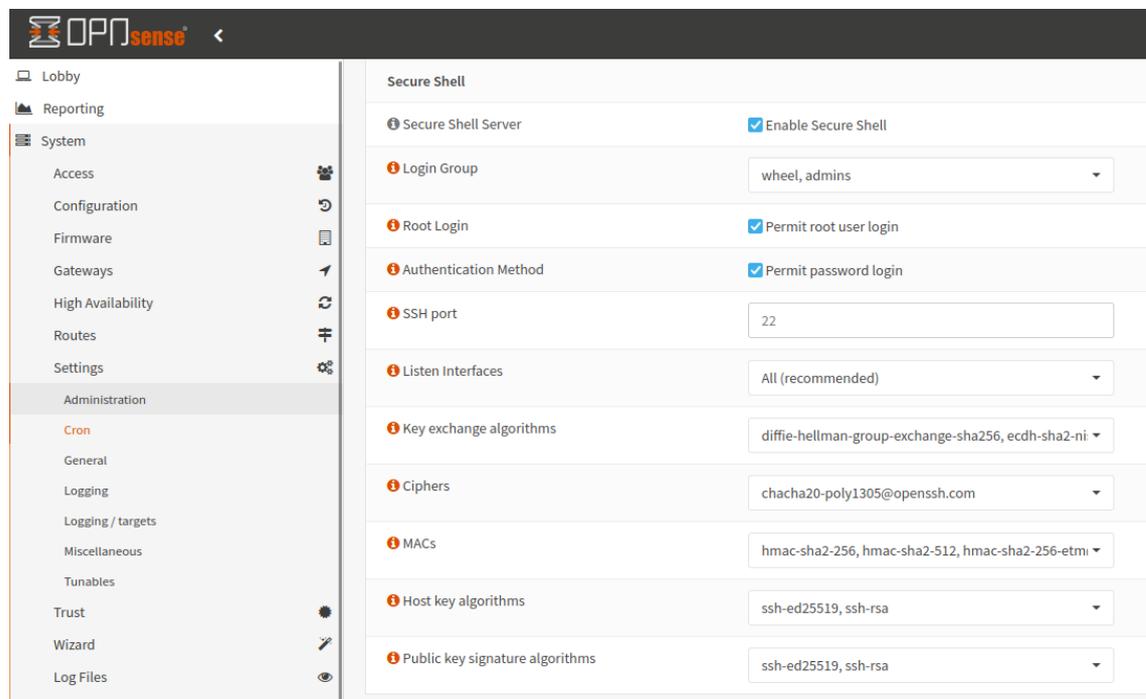


Figura 6 - Interfaz gráfica del producto – *System settings administration*

PARÁMETROS SECCIÓN WEB	
<i>Protocol</i>	HTTPS
<i>SSL Ciphers</i>	Ver Apartado 6.1 MODO DE OPERACIÓN SEGURO
<i>Enable HTTP Strict Transport Security</i>	Marcar
<i>Disable web GUI Redirect Rule</i>	Desmarcar
<i>Enable access log</i>	Marcar
<i>Listen interfaces</i>	Seleccionar interfaces conectados a redes seguras
<i>Disable HTTP_REFERER enforcement check</i>	Desmarcar

Tabla 6 – Parámetros sección Web

Figura 7 - Interfaz gráfica del producto. *Secure Shell*

PARÁMETROS SECCIÓN SECURE SHELL	
<b><i>Enable Secure Shell</i></b>	Marcar
<b><i>Login Group</i></b>	<i>wheel, admins</i>
<b><i>Permit root user login</i></b>	Desmarcar
<b><i>Permit password login</i></b>	Desmarcar (se necesitarán certificados digitales para el acceso por SSH)
<b><i>Listen interfaces</i></b>	Seleccionar interfaces conectados a redes seguras
<b><i>Show cryptographic overrides</i></b>	

PARÁMETROS SECCIÓN SECURE SHELL	
<b>Key exchange algorithms</b>	Ver Apartado 6.1 MODO DE OPERACIÓN SEGURO
<b>Ciphers</b>	Ver Apartado 6.1 MODO DE OPERACIÓN SEGURO
<b>MACs</b>	Ver Apartado 6.1 MODO DE OPERACIÓN SEGURO
<b>Host key algorithms</b>	ssh-ed-25519, ssh-rsa
<b>Public key signature algorithms</b>	Ver Apartado 6.1 MODO DE OPERACIÓN SEGURO

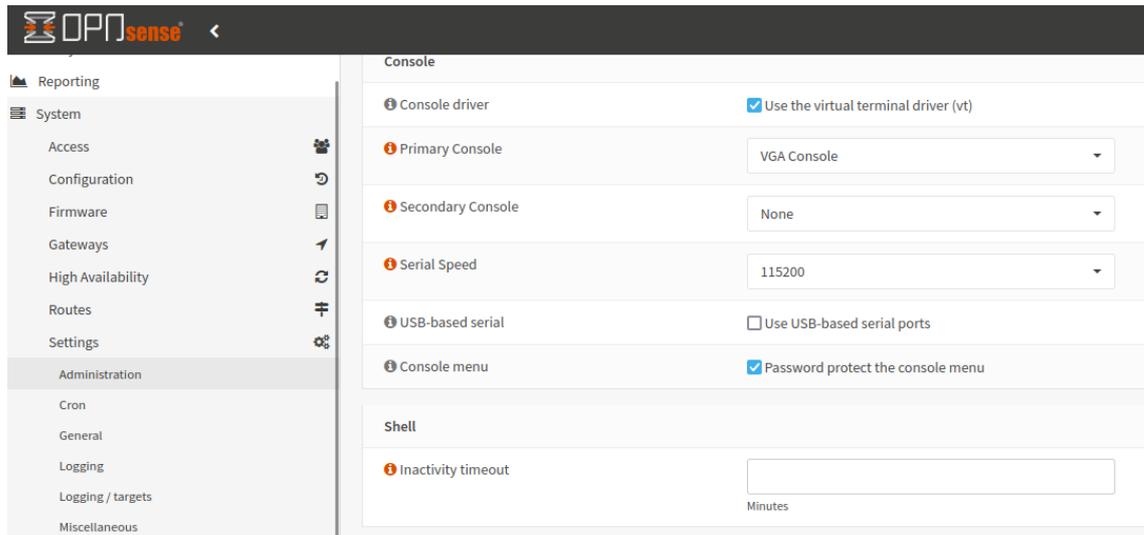
Tabla 7 – Parámetros sección *Secure Shell*

Figura 8 - Interfaz gráfica del producto. Administration tab

PARÁMETROS SECCIÓN CONSOLE	
<b>Password protect the console</b>	Marcar

Tabla 8 – Parámetros sección Console

PARÁMETROS SECCIÓN SHELL	
<b>Inactivity timeout</b>	Indicar el número de minutos tras los cuales una sesión de consola sin actividad cerrará la sesión. Se recomienda establecer este valor en 300 segundos (5 minutos).

Tabla 9 – Parámetros sección Shell

### 6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

51. 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.
52. 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> [REF21] con instrucciones al respecto y cómo reforzar la seguridad de dichas cuentas.
53. **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.
54. Para la autenticación con credenciales locales, a través de *System* → *Access* → *Servers* habrá que pulsar sobre el icono *Edit* y **establecer los siguientes valores para reforzar la seguridad de las contraseñas:**

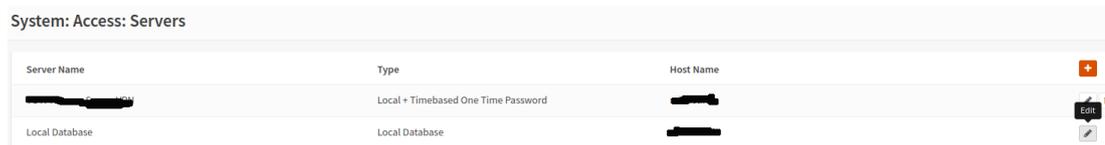


Figura 9 – System > Access > Servers

- *Policy – Enable password policy constraints* = Marcar para habilitar la política de robustez de contraseñas.
  - *Duration* = Elegir un valor de la lista distinto de “*Disable*”, para habilitar la vigencia máxima de la contraseña en días. Al alcanzar la vigencia máxima una contraseña, el sistema fuerza al usuario a modificarla para poder acceder. Se recomienda establecer un período máximo de vigencia de 60 días.
  - *Length* = 12 para forzar un tamaño mínimo de caracteres en las contraseñas.
  - *Complexity – Enable complexity requirements* = Marcar para requerir complejidad en las contraseñas. Se recomienda que la contraseña requiera el uso de letras mayúsculas, letras minúsculas, números y símbolos especiales.
55. Estas opciones aplican a la base de datos local de usuarios. Si se usan otros métodos de autenticación (LDAP o RADIUS, por ejemplo), será el proveedor de dicho mecanismo de autenticación quien dicte las características y opciones de complejidad que deben cumplir las contraseñas.
56. En cuanto a los parámetros de sesión, es posible gestionarlos en *System* → *Settings* → *Administración*:
- *Web GUI*, parámetro *Session Timeout* indica los minutos que tarda en expirar una sesión inactiva en la web de gestión, siendo por defecto 240 minutos. Se recomienda establecer un tiempo de inactividad de **5 minutos**.
  - *Shell*, parámetro *Inactivity timeout* indica los minutos que tarda en expirar una sesión inactiva de SSH o consola. Se recomienda establecer un tiempo de inactividad de **5 minutos**.

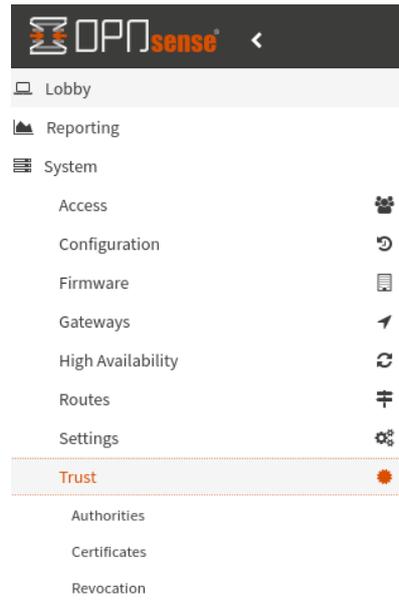
57. El número máximo de intentos fallidos de autenticación es configurable, siendo por defecto 5, con un tiempo de espera tras superar el umbral de 1 hora. Se recomienda establecer un límite de 3 intentos fallidos de autenticación, con un tiempo de espera de 5 minutos tras alcanzar el número establecido de intentos fallidos.

## 6.4 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> [REF17]. Se puede gestionar local o remotamente según se indica en el Apartado 6.2.1 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.
59. En la dirección <https://docs.opnsense.org/interfaces.html> [REF22] 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*).
60. Los interfaces permiten asignarles un nombre descriptivo y una descripción, así como una MAC e IP, así como habilitarlos o deshabilitarlos.
61. 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.

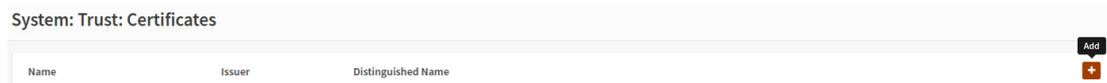
## 6.5 GESTIÓN DE CERTIFICADOS

62. Se realiza en la web de administración a través del menú *System* → *Trust*, donde se localizan los siguientes submenús:
- *Authorities*, para gestionar autoridades de certificados.
  - *Certificates*, para gestionar certificados.
  - *Revocation*, para gestionar revocaciones.



**Figura 10 - Interfaz gráfica. Trust Tab**

63. Para generar una solicitud de certificado (CSR), seleccionar System → Trust → Certificates y pulsamos el botón Add.



**Figura 11 - Interfaz gráfica. Añadir certificados**

64. En la pantalla que aparece:
- *Method* = Create a Certificate Signing Request.
  - *Descriptive name* = Nombre descriptivo que se quiere asignar a esta solicitud de certificado.
  - *Key Type* y *Key Length*. Las combinaciones aceptables a nivel de seguridad vienen indicadas en la tabla siguiente:

Figura 12 - Interfaz gráfica. Certificates tab

KEY TYPE	KEY LENGTH
<b>RSA</b>	<b>3072/4096/8192</b>
<b>Elliptic Curve</b>	<b>prime256v1/secp384r1</b>

Tabla 10 – Tipos y longitudes de clave

65. Para importar un certificado, ir a la misma pantalla que en el párrafo anterior, pero en *Method* habrá que seleccionar *Import an existing Certificate*. Habrá que agregar un nombre descriptivo al certificado que se desea importar, y rellenar los siguientes campos:

- *Certificate data* = Certificado emitido en formato X.509 PEM.
- *Private key data* = Clave privada del certificado en formato X.509 PEM.

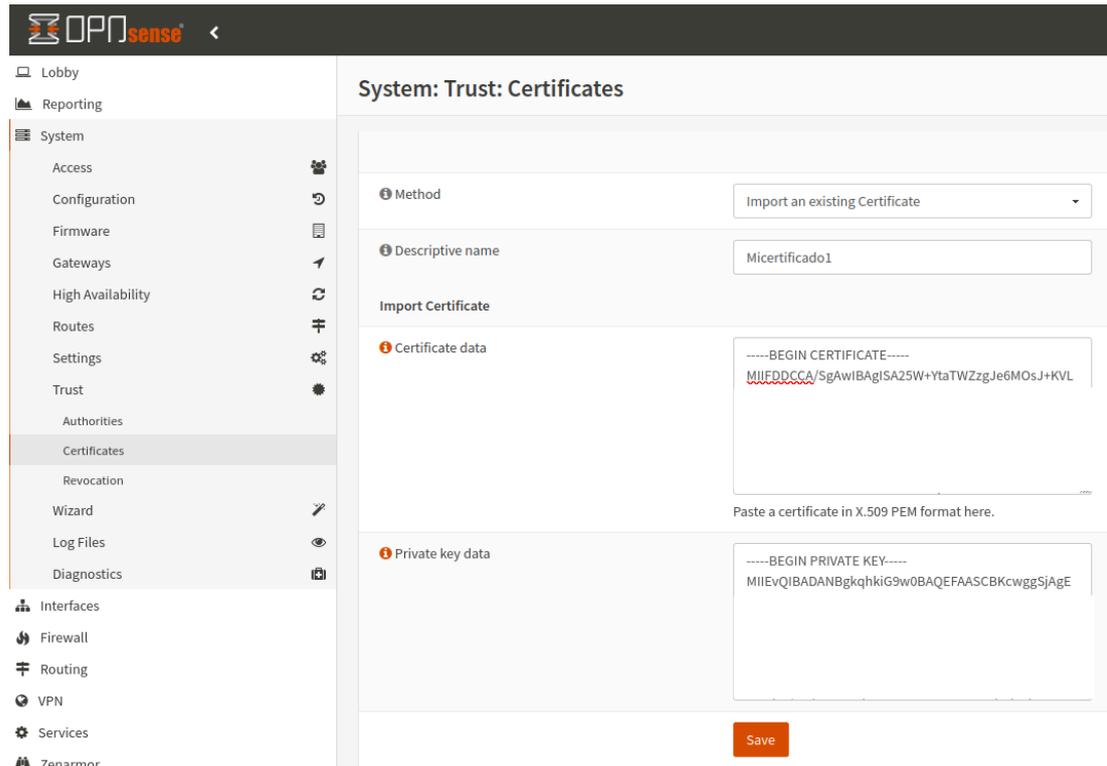


Figura 13 - Interfaz gráfica. Importando certificados

66. Si deseamos importar un certificado de CA raíz, ir a *System* → *Trust* → *Authorities*, y pulsar sobre el botón *Add*.

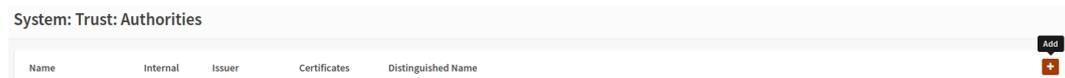


Figura 14 - Interfaz gráfica. Añadir certificados

67. En la pantalla aparecerá:
- *Method* = Import an existing Certificate Authority.
  - *Certificate data* = Certificado de la CA en formato X.509 PEM.
  - *Certificate Private Key* = Clave privada del certificado anterior. Opcional en la mayor parte de las ocasiones, pero necesaria si queremos generar una CRL.
68. OPNsense emplea para validar los certificados la vigencia de los mismos. Para aquellos servicios que usan certificados que emplean las Autoridades de Certificación configuradas en *System* → *Trust* → *Authorities* se puede crear o importar una Certificate Revocation List (CRL) donde consultar en tiempo real el estado actual de los certificados.

## 6.6 SERVIDORES DE AUTENTICACIÓN

69. OPNsense soporta como servidores externos de autenticación LDAP (*OpenLDAP*, MS Active Directory y Novell eDirectory) y *Radius*.
70. LDAP debe configurarse haciendo uso de protocolos de transporte seguros, en *System* → *Access* → *Servers*, seleccionando en el parámetro Transport los valores *StartTLS* o *SSL*.

*Encrypted.* En ambos casos se requerirá usar una CA privada definida previamente en *System* → *Trust* → *Authorities*.

71. Es necesario indicar que para emplear LDAP como método de autenticación, el firewall de OPNsense debe estar configurado, y ser capaz de acceder al servidor LDAP.
72. Para más información acerca del proceso a seguir para emplear un servidor LDAP como servidor de autenticación, se recomienda consultar el enlace: <https://docs.opnsense.org/manual/how-tos/user-ldap.html> [REF23]
73. **LDAP** permite configurarse adicionalmente con **TOTP**, puede consultarse [https://docs.opnsense.org/manual/two\\_factor.html](https://docs.opnsense.org/manual/two_factor.html) [REF19].
74. Para usar **Radius**, se recomienda dirigir el tráfico al puerto definido en el servidor (por defecto 1812) mediante un protocolo seguro, por ejemplo, a través de una VPN.
75. Para más información acerca del proceso de configuración de un servidor Radius como método de autenticación, se recomienda consultar el siguiente enlace: <https://docs.opnsense.org/manual/how-tos/user-radius.html> [REF24]

## 6.7 SINCRONIZACIÓN

76. 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> [REF25].
77. Por defecto, el producto está configurado para emplear los servidores NTP de Opnsense: `<X.opnsense.pool.ntp.org>`
78. La siguiente tabla muestra algunas de las opciones que pueden ser configuradas:

<b>Interface(s)</b>	<i>Interfaces to bind to, when none is selected it listens to all</i>
<b>Time servers</b>	<p><i>Servers to use, comes with two toggles:</i></p> <ul style="list-style-type: none"> <li>• <b>Prefer</b> <i>Marks the server as preferred.</i></li> <li>• <b>Do not use</b> <i>Marks the server as unused, except for display purposes. The server is discarded by the selection algorithm</i></li> </ul>
<b>Orphan mode</b>	<i>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.</i>
<b>NTP graphs</b>	<i>Enable RRD graphs of NTP statistics, which can be viewed in Reporting ▶ Health</i>

<b>Syslog logging</b>	<i>Extend logging with peer and/or system messages</i>
<b>Statistics logging</b>	<i>Enable statistical logging in /var/log/ntp, doesn't come with a user interface</i>
<b>Access restrictions</b>	<i>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.</i>
<b>Leap seconds</b>	<i>You can manually supply ntpd with a leap seconds file, more detailed info on the contents of those files can be found here</i>

Tabla 11 – Opciones de configuración de NTP

79. La configuración de dicho servicio se hará mediante el interfaz web de administración, acorde al uso recomendado del mismo en el presente procedimiento de uso.
80. NTP está deshabilitado si no hay servidores de tiempo configurados.

## 6.8 ACTUALIZACIONES

81. **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*. 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> [REF26].
82. 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.

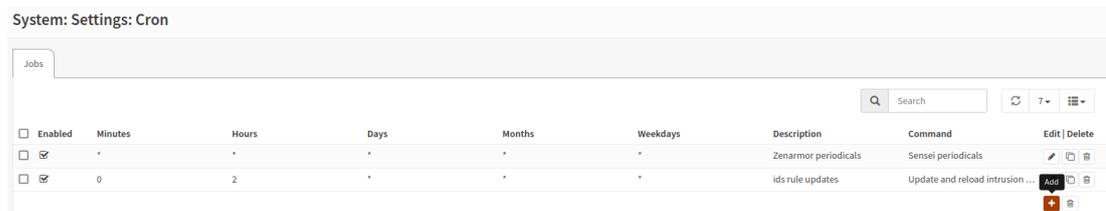


Figura 15 - Interfaz gráfica. Cron tab

The screenshot shows the 'Edit job' configuration window. The 'enabled' checkbox is checked. The 'Minutes', 'Hours', 'Day of the month', 'Months', and 'Days of the week' fields are all set to '\*'. The 'Command' dropdown menu is set to 'Automatic firmware update'. Below the dropdown, there is a 'Clear All' button and a 'Parameters' field containing 'Automatic firmware update'. The 'Description' field is empty. At the bottom right, there are 'Cancel' and 'Save' buttons.

Figura 16 - Interfaz gráfica. Activando las actualizaciones automáticas

83. Para más información acerca del proceso de instalación de actualización, se recomienda consultar el siguiente enlace: <https://docs.opnsense.org/manual/updates.html> [REF26]

## 6.9 AUTO-CHEQUEOS

84. 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 siguientes, tal y como se muestra en la imagen siguiente:

Figura 17 - Interfaz gráfica. 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.
85. 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.
86. Para más información al respecto, se recomienda consultar el enlace: <https://docs.opnsense.org/security.html> [REF37]

## 6.10 ALTA DISPONIBILIDAD

87. El software utiliza el protocolo libre *Common Address Redundancy Protocol (CARP)* [REF28] 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.
88. 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.

89. La configuración se realiza a través del menú *System* → *High Availability* → *Settings*.
90. Los detalles de la configuración y opciones recomendadas pueden consultarse en la dirección <https://docs.opnsense.org/manual/hacarp.html> [REF27].
91. Asimismo, se recomienda consultar el siguiente enlace:  
<https://docs.opnsense.org/manual/how-tos/carp.html> [REF28].

## 6.11 AUDITORÍA

### 6.11.1 REGISTRO DE EVENTOS

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

TIPO DE EVENTO	ACCESIBLE EN...	DESCRIPCIÓN
<i>System Log</i>	<i>System</i> → <i>Log Files</i> → <i>General</i>	Eventos del propio sistema
<i>Audit</i>	<i>System</i> → <i>Log Files</i> → <i>Audit</i>	Acciones de los usuarios
<i>Backend / config daemon</i>	<i>System</i> → <i>Log Files</i> → <i>Backend</i>	Eventos de generación de configuraciones por el uso de la API
<i>Web GUI</i>	<i>System</i> → <i>Log Files</i> → <i>Web GUI</i>	Eventos del propio servidor web que publica la interfaz web de administración (Lighttpd)
<i>Firmware</i>	<i>System</i> → <i>Firmware</i> → <i>Log File</i>	Eventos de actualizaciones del sistema
<i>Gateways</i>	<i>System</i> → <i>Gateways</i> → <i>Log File</i>	Eventos relativos al seguimiento de puertos de enlace de Dpinger
<i>Routing</i>	<i>System</i> → <i>Routes</i> → <i>Log File</i>	Eventos de interfaces o cambios de rutas

**Tabla 12 – Tipos de eventos Syslog**

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

System: Log Files: General

Date	Facility	Severity	Process	PID	Line
2022-09-22T14:26:28	1	Error	opnsense	42663	/usr/local/etc/rc.routing_configure: Removing static route for monitor 8.8.8.8 via [REDACTED]
2022-09-22T14:26:28	1	Error	opnsense	42663	/usr/local/etc/rc.routing_configure: ROUTING: keeping current default gateway [REDACTED]
2022-09-22T14:26:28	1	Error	opnsense	42663	/usr/local/etc/rc.routing_configure: ROUTING: setting IPv4 default route to [REDACTED]
2022-09-22T14:26:28	1	Error	opnsense	42663	/usr/local/etc/rc.routing_configure: ROUTING: IPv4 default gateway set to wan
2022-09-22T14:26:28	1	Error	opnsense	42663	/usr/local/etc/rc.routing_configure: ROUTING: entering configure using defaults
2022-09-22T14:26:28	1	Error	opnsense	41766	/usr/local/etc/rc.newwanip: Interface " (ovpn2) is disabled or empty, nothing to do.
2022-09-22T14:26:28	1	Error	opnsense	41766	/usr/local/etc/rc.newwanip: IPv4 renewal is starting on 'ovpn2'
2022-09-22T14:26:27	1	Error	opnsense	65426	/usr/local/etc/rc.newwanip: IP renewal deferred during boot on 'ovpn2'
2022-09-22T14:26:24	1	Error	opnsense	59584	/usr/local/etc/rc.syshook.d/carp/20-openvpn: Resyncing OpenVPN instances for interface IP CARP [REDACTED]
2022-09-22T14:26:24	1	Error	opnsense	59584	/usr/local/etc/rc.syshook.d/carp/20-openvpn: Carp cluster member "IP CARP [REDACTED]" has resumed the state "BACKUP" for vhid 247
2022-09-22T14:26:23	1	Error	opnsense	46394	/usr/local/etc/rc.syshook.d/carp/20-openvpn: Resyncing OpenVPN instances for interface IP CARP [REDACTED]
2022-09-22T14:26:23	1	Error	opnsense	46394	/usr/local/etc/rc.syshook.d/carp/20-openvpn: Carp cluster member "IP CARP [REDACTED]" has resumed the state "BACKUP" for vhid 246

Showing 21 to 31

Clear log

Figura 18 - Interfaz gráfica. Eventos

94. Pulsando el icono , descargará un fichero de texto con los eventos mostrados según el filtro activo.
95. Los campos para todos los tipos de evento son:
  - *Date* = fecha y hora en la que se produce el evento.
  - *Facility* = Número entre 0 y 23 inclusive, definido en RFC5424.
  - *Severity* = Número entre 0 y 7 inclusive, definido en RFC5424.
  - *Process* = Nombre del proceso que origina el evento.
  - *PID* = Identificador del proceso que genera el evento.
  - *Line* = Texto del evento.

## 6.12 ALMACENAMIENTO LOCAL

96. El sistema almacena internamente los registros de los eventos de forma predeterminada, en la carpeta del sistema `/var/log`.
97. En caso de alcanzar el límite del almacenamiento interno, el sistema sobrescribirá los registros más antiguos.

### 6.12.1 ALMACENAMIENTO REMOTO

98. 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.



**Figura 19 - Interfaz gráfica. Almacenamiento remoto**

99. Es posible obtener más información a través del enlace:

<https://docs.opnsense.org/manual/settingsmenu.html#logging-targets>

100. 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.

101. Para más información al respecto, se recomienda consultar el siguiente enlace: <https://docs.opnsense.org/manual/settingsmenu.html> [REF29].

### 6.13 BACKUP

102. Es posible realizar copias de la configuración completa del sistema a través del menú *System* → *Configuration* → *Backups* pulsando sobre el botón “*Download configuration*”. Dicha copia se puede cifrar marcando la opción “*Encrypt this configuration file*”. Se recomienda almacenar regularmente ficheros cifrados con las copias de seguridad en lugar seguro, cumpliendo la normativa al efecto.

103. Se puede recuperar la configuración completa del sistema, o de servicios concretos del mismo, mediante el botón “*Restore configuration*”, y seleccionando el fichero de backup a cargar.

**System: Configuration: Backups**

**Download**

Do not backup RRD data.  
 Encrypt this configuration file.

Password

Confirmation

**Download configuration**

Click this button to download the system configuration in XML format.

**Restore**

Restore area:  
 ALL

No se ha seleccionado ningún archivo.

Reboot after a successful restore.  
 Configuration file is encrypted.

**Restore configuration**

Open a configuration XML file and click the button below to restore the configuration.

**Figura 20 - Interfaz gráfica. Configuración de backups**

104. Es posible configurar la realización de **copias en la nube**. Los detalles de dicha configuración pueden consultarse en la dirección [https://docs.opnsense.org/manual/how-tos/cloud\\_backup.html](https://docs.opnsense.org/manual/how-tos/cloud_backup.html) [REF30].
105. Además, OPNsense almacena un historial de los cambios producidos en la configuración. Dicho historial es accesible a través de *System* → *Configuration* → *History*. Por defecto almacena los últimos 60 cambios en la configuración, siendo esto parametrizable, y permite de forma fácil revertir cualquiera de los cambios o descargar la configuración que tenía el sistema en ese momento.
106. Se recomienda llevar a cabo copias de seguridad de forma periódica.

## 6.14 SERVICIOS DE SEGURIDAD

107. 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> [REF31].
108. 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.
109. Mediante *System* → *Firewall* → *Alias* 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/alias.html> [REF32]

110. 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*.
111. 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.
112. 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> [REF33]
113. 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.
114. 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.
115. Los parámetros más importantes de una regla son:

PARÁMETROS PRINCIPALES DE UNA REGLA DE CORTAFUEGOS	
<b>Action</b>	Acción a efectuar con el paquete si aplica esta regla: <i>Pass</i> = Se permite al paquete continuar <i>Reject</i> = Se impide al paquete continuar y se remite al origen del mismo un paquete indicándolo <i>Block</i> = Se impide al paquete continuar
<b>Disabled</b>	Si la regla está desactivada. Por defecto desmarcado.
<b>Quick</b>	Si la regla se aplica inmediatamente. Por defecto marcado
<b>Interface</b>	Interfaz o interfaces donde se aplica la regla
<b>Direction</b>	Dirección del tráfico: - <i>in</i> = entrando al interfaz (por defecto)

PARÁMETROS PRINCIPALES DE UNA REGLA DE CORTAFUEGOS	
<b>TCP/IP Version</b>	- <i>out</i> = saliendo del interfaz - <i>any</i> = entrando y saliendo del interfaz Versión del protocolo IP en la que aplica: IPv4, IPv6 o IPv4+IPv6
<b>Protocol</b>	Protocolo IP en el que aplica: any, TCP, UDP, TCP/UDP o ICMP
<b>Source</b>	Origen del tráfico
<b>Destination</b>	Destino del tráfico
<b>Destination port range</b>	Puerto o rango de puertos en el destino donde se dirige el tráfico
<b>Log</b>	Si queremos que la regla emita un registro de evento cuando aplique a tráfico
<b>Category</b>	Categoría a la que pertenece la regla
<b>Description</b>	Texto descriptivo

Tabla 13 – Parámetros principales de una regla de cortafuegos

116. 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	
<b>Action</b>	Pass
<b>Disabled</b>	Desmarcar
<b>Quick</b>	Marcar
<b>Interface</b>	LAN
<b>Direction</b>	in
<b>TCP/IP Version</b>	IPv4
<b>Protocol</b>	TCP
<b>Source</b>	EquipoOrigen
<b>Destination</b>	EquipoDestino
<b>Destination port range – from</b>	1433
<b>Destination port range – to</b>	1433
<b>Log</b>	Marcar

Tabla 14 – Ejemplo de regla para permitir tráfico

117. 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.
118. 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.
119. 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](https://docs.opnsense.org/manual/firewall_settings.html#schedules) [REF35].
120. 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](https://docs.opnsense.org/manual/firewall_scrub.html) [REF36].

## 7. FASE DE OPERACIÓN

121. Una vez instalado y configurado el sistema, los **procedimientos operativos** a llevar a cabo durante la fase de operación y mantenimiento del producto son:

- a) **Comprobaciones periódicas del *hardware* y *software*** para asegurar que no se ha introducido hardware o software no autorizado
- b) **Verificaciones periódicas del *firmware*** activo y su integridad, con objeto de comprobar que está libre de software malicioso.
- c) Aplicación regular de **actualizaciones y parches** de seguridad, para mantener una configuración segura.
- d) Realización periódica de **copias de seguridad** y almacenamiento de forma centralizada de las mismas, separadas del sistema en funcionamiento y en ficheros encriptados.
- e) Envío de información de auditoría a un servidor **Syslog remoto**, así como copias de seguridad cifradas del mismo, que se guardarán en las condiciones y por el periodo establecido en la normativa de seguridad
- f) **Auditoría de los eventos** especificados en la normativa de referencia y aquellos otros extraídos del análisis de riesgos.

## 8. CHECKLIST

122. Se presenta una **lista de comprobación** de las recomendaciones de seguridad descritas en el presente documento:

ACCIONES	SÍ	NO	OBSERVACIONES
<b>DESPLIEGUE E INSTALACIÓN</b>			
Verificación de la <b>entrega segura</b> del producto	<input type="checkbox"/>	<input type="checkbox"/>	<a href="https://docs.opnsense.org/manual/install.all.html">https://docs.opnsense.org/manual/install.all.html</a> , "Download and verification"
Instalación en un <b>entorno seguro</b>	<input type="checkbox"/>	<input type="checkbox"/>	
<b>Actualización</b> de firmware	<input type="checkbox"/>	<input type="checkbox"/>	
<b>CONFIGURACIÓN</b>			
<b>MODO DE OPERACIÓN SEGURO</b>			
Reforzar <b>seguridad</b> en arranque	<input type="checkbox"/>	<input type="checkbox"/>	
Sustituir OpenSSL por <b>LibreSSL</b>	<input type="checkbox"/>	<input type="checkbox"/>	
Sustituir <b>certificado</b> auto-firmado	<input type="checkbox"/>	<input type="checkbox"/>	
Cambiar <b>clave</b> por defecto de <b>root</b>	<input type="checkbox"/>	<input type="checkbox"/>	
Habilitar parámetro " <b>Enable access log</b> "	<input type="checkbox"/>	<input type="checkbox"/>	
Crear <b>dos reglas</b> de cortafuegos para evitar <b>ataques DoS</b>	<input type="checkbox"/>	<input type="checkbox"/>	
<b>Evitar</b> ataques de <b>degradación TLS</b> en comunicaciones con <b>Syslog externo</b>	<input type="checkbox"/>	<input type="checkbox"/>	
Configuración de <b>suites de cifrado</b> aceptadas y parámetros de las mismas	<input type="checkbox"/>	<input type="checkbox"/>	
Configurar <b>TLS</b> para comunicar con <b>Syslog externo</b>	<input type="checkbox"/>	<input type="checkbox"/>	
<b>AUTENTICACIÓN</b>			
Configurar autenticación de doble factor ( <b>2FA</b> )	<input type="checkbox"/>	<input type="checkbox"/>	<a href="https://docs.opnsense.org/manual/two_factor.html">https://docs.opnsense.org/manual/two_factor.html</a>
<b>Minimizar</b> uso <b>claves precompartidas</b>	<input type="checkbox"/>	<input type="checkbox"/>	

ACCIONES	SÍ	NO	OBSERVACIONES
<b>ADMINISTRACIÓN LOCAL Y REMOTA</b>			
Reforzar <b>seguridad</b> en el acceso	<input type="checkbox"/>	<input type="checkbox"/>	
<b>CONFIGURACIÓN DE ADMINISTRADORES</b>			
Crear <b>cuentas alternativas</b> de administración con los privilegios mínimos requeridos	<input type="checkbox"/>	<input type="checkbox"/>	<a href="https://docs.opnsense.org/manual/how-tos/user-local.html">https://docs.opnsense.org/manual/how-tos/user-local.html</a>
Incrementar <b>robustez contraseñas</b>	<input type="checkbox"/>	<input type="checkbox"/>	
Configurar <b>parámetros de contraseñas</b> locales	<input type="checkbox"/>	<input type="checkbox"/>	
Modificar <b>parámetros de sesión</b>	<input type="checkbox"/>	<input type="checkbox"/>	
<b>CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS</b>			
Asignar <b>interfaz de gestión</b>	<input type="checkbox"/>	<input type="checkbox"/>	<a href="https://docs.opnsense.org/manual/install.html#initial-configuration">https://docs.opnsense.org/manual/install.html#initial-configuration</a>
Marcar <b>“Block private networks”</b> y <b>“Block bogon networks”</b>	<input type="checkbox"/>	<input type="checkbox"/>	En las interfaces donde sea posible según el direccionamiento y flujos de tráfico
<b>CONFIGURACIÓN DE PROTOCOLOS SEGUROS</b>			
Sustituir OpenSSL por <b>LibreSSL</b>	<input type="checkbox"/>	<input type="checkbox"/>	Algunos plugins solo funciona con OpenSSL
<b>Parametrizar</b> los distintos tipos de VPN	<input type="checkbox"/>	<input type="checkbox"/>	En caso de que hagamos uso de alguna
<b>GESTIÓN DE CERTIFICADOS</b>			
Configurar propiedades <b>“Key Type”</b> y <b>“Key Length”</b>	<input type="checkbox"/>	<input type="checkbox"/>	Cuando hagamos una CSR para solicitar un certificado
<b>SERVIDORES DE AUTENTICACIÓN</b>			
Configurar parámetro <b>“Transport”</b> para servidor <b>LDAP</b>	<input type="checkbox"/>	<input type="checkbox"/>	Si vamos a usar un servidor de autenticación externo LDAP
Configurar <b>TOTP</b>	<input type="checkbox"/>	<input type="checkbox"/>	Si vamos a usar un servicio que permita el TOTP
Configurar <b>Radius</b> para comunicarse a través de una VPN	<input type="checkbox"/>	<input type="checkbox"/>	Si vamos a usar un servidor de autenticación externo Radius

ACCIONES	SÍ	NO	OBSERVACIONES
<b>SINCRONIZACIÓN HORARIA</b>			
Configurar <b>servidor NTP</b>	<input type="checkbox"/>	<input type="checkbox"/>	<a href="https://docs.opnsense.org/manual/ntp.html?highlight=ntp">https://docs.opnsense.org/manual/ntp.html?highlight=ntp</a>
<b>ACTUALIZACIONES</b>			
<b>Actualizar</b> el sistema	<input type="checkbox"/>	<input type="checkbox"/>	<a href="https://docs.opnsense.org/manual/firmware.html#updates">https://docs.opnsense.org/manual/firmware.html#updates</a>
<b>Programar actualizaciones</b> automáticas del firmware	<input type="checkbox"/>	<input type="checkbox"/>	Una vez configurado en alta disponibilidad para evitar cortes de servicio
<b>AUTO-CHEQUEOS</b>			
<b>Realizar</b> los chequeos del sistema	<input type="checkbox"/>	<input type="checkbox"/>	
<b>SNMP</b>			
Instalar plugin <b>os-net-snmp</b>	<input type="checkbox"/>	<input type="checkbox"/>	
Configurar servidor <b>SNMPv3 remoto</b>	<input type="checkbox"/>	<input type="checkbox"/>	
Crear <b>usuarios SNMPv3</b>	<input type="checkbox"/>	<input type="checkbox"/>	
<b>ALTA DISPONIBILIDAD</b>			
Crear direcciones IP virtuales <b>CARP</b> para cada interfaz pertinente en cada nodo del cluster	<input type="checkbox"/>	<input type="checkbox"/>	<a href="https://docs.opnsense.org/manual/firewall_vip.html">https://docs.opnsense.org/manual/firewall_vip.html</a>
Configurar y <b>verificar</b> el cluster <b>activo-pasivo</b>	<input type="checkbox"/>	<input type="checkbox"/>	<a href="https://docs.opnsense.org/manual/hacarp.html">https://docs.opnsense.org/manual/hacarp.html</a>
<b>AUDITORÍA</b>			
Configurar <b>syslog-ng</b> para enviar la información de auditoría de forma segura a servidor syslog remoto	<input type="checkbox"/>	<input type="checkbox"/>	
<b>BACKUP</b>			
<b>Almacenamiento</b> de copias de seguridad encriptadas	<input type="checkbox"/>	<input type="checkbox"/>	Cumpliendo la normativa al efecto
Configuración de almacenamiento de copias de seguridad <b>en la nube</b>	<input type="checkbox"/>	<input type="checkbox"/>	Si la nube cumple la normativa al efecto

ACCIONES	SÍ	NO	OBSERVACIONES
<b>FASE DE OPERACIÓN</b>			
<b>Comprobación</b> periódica del <b>hardware y software</b>	<input type="checkbox"/>	<input type="checkbox"/>	
<b>Verificaciones</b> periódicas del <b>firmware</b> activo y su integridad	<input type="checkbox"/>	<input type="checkbox"/>	
Aplicación regular de <b>actualizaciones y parches</b> de seguridad	<input type="checkbox"/>	<input type="checkbox"/>	
Realización periódica de <b>copias de seguridad</b> y almacenamiento de las mismas	<input type="checkbox"/>	<input type="checkbox"/>	
Envío de información de auditoría a servidor <b>Syslog remoto</b>	<input type="checkbox"/>	<input type="checkbox"/>	
<b>Auditoría de los eventos</b> indicados pro la normativa y aquellos extraídos del análisis de riesgos	<input type="checkbox"/>	<input type="checkbox"/>	

## 9. REFERENCIAS

123. A continuación, indicamos la **documentación referenciada** en la presente guía:

- REF1** Web oficial del fabricante  
<https://opnsense.org>
- REF2** Documentación oficial del fabricante  
<https://docs.opnsense.org>
- REF3** LibreSSL  
<https://en.wikipedia.org/wiki/LibreSSL>
- REF4** Guía CCN-STIC-807  
<https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/513-ccn-stic-807-criptologia-de-empleo-en-el-ens/file.html>
- REF5** RFC 6238: TOTP: Time-Based One-Time Password Algorithm  
<https://www.rfc-editor.org/rfc/rfc6238>
- REF6** RFC 5424: The Syslog Protocol  
<https://www.rfc-editor.org/rfc/rfc5424>
- REF7** RFC 2741: IPv6 Testing Address Allocation  
<https://www.rfc-editor.org/rfc/rfc2741>
- REF8** RFC 1918: Address Allocation for Private Internets  
<https://www.rfc-editor.org/rfc/rfc1918>
- REF9** Suricata  
<https://suricata.io/>
- REF10** Netmap  
<https://manpages.ubuntu.com/manpages/bionic/man4/netmap.4freebsd.html>
- REF11** Página de descarga de OPNsense  
<https://opnsense.org/download/>
- REF12** OPNsense Instalación inicial y configuración  
<https://docs.opnsense.org/manual/install.html>
- REF13** OPNsense Legal Notices  
<https://opnsense.org/about/legal-notices/>
- REF14** OPNsense Hardware Sizing and Setup  
<https://docs.opnsense.org/manual/hardware.html>
- REF15** OPNsense Virtual and Cloud-based Installation  
<https://docs.opnsense.org/manual/virtuals.html>
- REF16** OPNsense Installation Method  
<https://docs.opnsense.org/manual/install.html#installation-method>
- REF17** OPNsense Initial Configuration  
<https://docs.opnsense.org/manual/install.html#initial-configuration>

- REF18** *OPNsense Setup Guides*  
<https://docs.opnsense.org/setup.html#setup-guides>
- REF19** *OPNsense Two-Factor Authentication*  
[https://docs.opnsense.org/manual/two\\_factor.html](https://docs.opnsense.org/manual/two_factor.html)
- REF20** *OPNsense Authentication*  
<https://docs.opnsense.org/manual/users.html#authentication>
- REF21** *OPNsense User Management - Users and Groups*  
<https://docs.opnsense.org/manual/how-tos/user-local.html>
- REF22** *OPNsense Interfaces*  
<https://docs.opnsense.org/interfaces.html>
- REF23** *OPNsense LDAP*  
<https://docs.opnsense.org/manual/how-tos/user-ldap.html>
- REF24** *OPNsense RADIUS*  
<https://docs.opnsense.org/manual/how-tos/user-radius.html>
- REF25** *OPNsense - Network Time*  
<https://docs.opnsense.org/manual/ntpd.html?highlight=ntp>
- REF26** *OPNsense – Updates*  
<https://docs.opnsense.org/manual/firmware.html#updates>
- REF27** *OPNsense - High Availability*  
<https://docs.opnsense.org/manual/hacarp.html>
- REF28** *OPNsense – CARP*  
<https://docs.opnsense.org/manual/how-tos/carp.html>
- REF29** *OPNsense - System Settings*  
<https://docs.opnsense.org/manual/settingsmenu.html>
- REF30** *OPNsense - Cloud Backup*  
[https://docs.opnsense.org/manual/how-tos/cloud\\_backup.html](https://docs.opnsense.org/manual/how-tos/cloud_backup.html)
- REF31** *OPNsense – Firewall*  
<https://docs.opnsense.org/firewall.html>
- REF32** *OPNsense – Aliases*  
<https://docs.opnsense.org/manual/aliases.htm>
- REF33** *OPNsense – NAT*  
<https://docs.opnsense.org/manual/nat.html>
- REF34** *OPNsense – Spamhaus*  
<https://docs.opnsense.org/manual/how-tos/edrop.html>
- REF35** *OPNsense – Schedules*  
[https://docs.opnsense.org/manual/firewall\\_settings.html#schedules](https://docs.opnsense.org/manual/firewall_settings.html#schedules)

- REF36** *OPNsense - Firewall Normalization*  
[https://docs.opnsense.org/manual/firewall\\_scrub.html](https://docs.opnsense.org/manual/firewall_scrub.html)
- REF37** *OPNsense – Security*  
<https://docs.opnsense.org/security.html>

## 10. ABREVIATURAS

<b>2FA</b>	<i>Two Factor Authentication</i>
<b>BSD</b>	<i>Berkeley Software Distribution</i>
<b>CARP</b>	<i>Common Address Redundancy Protocol</i>
<b>CRL</b>	<i>Certificate Revocation List</i>
<b>CSR</b>	<i>Certificate Signing Request</i>
<b>CVE</b>	<i>Common Vulnerabilities and Exposures</i>
<b>ENS</b>	<i>Esquema Nacional de Seguridad</i>
<b>GIF</b>	<i>Generic tunneling Interface</i>
<b>GRE</b>	<i>Generic Routing Encapsulation</i>
<b>HTTPS</b>	<i>Hypertext Transfer Protocol Secure</i>
<b>IANA</b>	<i>Internet Assigned Numbers Authority</i>
<b>IKE</b>	<i>Internet Key Exchange</i>
<b>IP</b>	<i>Internet Protocol</i>
<b>IPsec</b>	<i>Internet Protocol security</i>
<b>IPv4</b>	<i>Internet Protocol version 4</i>
<b>IPv6</b>	<i>Internet Protocol versin 6</i>
<b>LAGG</b>	<i>Link Aggregation</i>
<b>LDAP</b>	<i>Lighweigt Directory Access Protocol</i>
<b>MAC</b>	<i>Media Access Control</i>
<b>NTP</b>	<i>Network Time Protocol</i>
<b>OID</b>	<i>Object IDentifier</i>
<b>OSI</b>	<i>Open System Interconnection</i>
<b>Radius</b>	<i>Remote Authentication Dial-In User Service</i>
<b>RFC</b>	<i>Request for Comments</i>
<b>RSA</b>	<i>Rivest, Shamir y Adleman</i>
<b>SNMP</b>	<i>Simple Network Management Protocol</i>
<b>SSH</b>	<i>Secure Shell</i>
<b>SSL</b>	<i>Secure Sockets Layer</i>
<b>TCP</b>	<i>Transmission Control Protocol</i>
<b>TLS</b>	<i>Transport Layer Security</i>
<b>TOTP</b>	<i>Time-based One-Time Password</i>
<b>UDP</b>	<i>User Datagram Protocol</i>
<b>VLAN</b>	<i>Virtual LAN</i>
<b>VPN</b>	<i>Virtual Private Network</i>
<b>VXLAN</b>	<i>Virtual Extensible LAN</i>

