



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

cpage.mpr.gob.es

Edita:



Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2022
NIPO: 083-22-175-0.

Fecha de Edición: junio de 2022

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

1. INTRODUCCIÓN	4
2. OBJETO Y ALCANCE	5
3. ORGANIZACIÓN DEL DOCUMENTO	6
4. FASE PREVIA A LA INSTALACIÓN	7
4.1 ENTREGA SEGURA DEL PRODUCTO	7
4.2 ENTORNO DE INSTALACIÓN SEGURO	7
4.3 REGISTRO DE UNIDAD	7
4.4 CONSIDERACIONES PREVIAS	9
4.4.1 MODO DE FUNCIONAMIENTO DEL PROXY	9
4.4.2 ENRUTAMIENTO	12
4.4.3 ALTA DISPONIBILIDAD	13
4.4.4 OPTIMIZACIÓN WAN	14
4.4.5 AUTENTICACIÓN	15
4.4.6 WEB CACHING	18
4.4.7 SERVICIO DE ANÁLISIS DE CONTENIDO	19
5. FASE DE INSTALACIÓN	21
5.1 PRIMER ACCESO AL DISPOSITIVO	21
5.2 INSTALACIÓN DEL FIRMANTE	21
5.2.1 HABILITACIÓN MODO FIPS	21
5.3 ACCESO A BIOS	23
6. FASE DE CONFIGURACIÓN.....	24
6.1 MODO DE OPERACIÓN SEGURO	24
6.2 CERTIFICADOS	25
6.3 ADMINISTRACIÓN DEL DISPOSITIVO	27
6.3.1 ADMINISTRACIÓN HTTPS (GUI)	28
6.3.2 CONFIGURACIÓN DE SSH	30
6.3.3 POLÍTICA DE CONTRASEÑAS.....	30
6.3.4 PARÁMETROS DE SESIÓN	32
6.3.5 USUARIO “ADMIN”	33
6.3.6 MENSAJE DE AVISO Y CONSENTIMIENTO	34
6.4 USUARIO MAINTAINER	35
6.5 CONFIGURACIÓN DE INTERFACES.....	35
6.6 CONFIGURACIÓN DE SERVICIOS DEL DISPOSITIVO	37
6.7 SERVIDORES DE AUTENTICACIÓN	38
6.7.1 SERVIDORES SINGLE SIGN-ON	38
6.7.2 SERVIDORES LDAP	40
6.7.3 SERVIDORES RADIUS	41
6.7.4 SERVIDORES TACACS+	42
6.7.5 KERBEROS	44
6.8 SINCRONIZACIÓN AUTOMÁTICA DEL RELOJ	45
6.9 BACKUP DE LA CONFIGURACIÓN	46
6.10 AUTO-CHEQUEOS.....	47

6.11	POLÍTICAS DE SEGURIDAD DEL PROXY	48
6.12	PERFILES DE SEGURIDAD	51
6.12.1	ANTIVIRUS	52
6.12.2	FILTRADO WEB	54
6.12.3	CONTROL DE APLICACIONES	56
6.12.4	PROTECCIÓN FRENTE A INTRUSIONES (IPS)	57
6.12.5	DLP	60
6.12.6	CONTENT ANALYSIS	61
6.12.7	INSPECCIÓN DEL TRÁFICO SSH/SSL	62
6.12.8	FILTRADO DNS	63
6.13	VPN	65
6.13.1	VPN IPSEC	65
6.13.2	VPN SSL	69
6.14	REGISTRO DE EVENTOS (LOGGING)	72
6.14.1	FORTIANALYZER	74
6.14.2	SYSLOG	76
7.	FASE DE OPERACIÓN	77
8.	CHECKLIST	78
9.	REFERENCIAS	79
10.	ABREVIATURAS	80

1. INTRODUCCIÓN

1. FortiProxy *Appliances* son dispositivos diseñados para proporcionar servicios de protección y control de navegación web de nueva generación, asegurando dicha protección en redes IPv4 (*Internet Protocol version 4*) e IPv6 (*Internet Protocol version 6*).
2. Ofrecen un potente filtrado que aúna las funcionalidades de filtrado web, filtrado DNS y control de aplicaciones.
3. Además, los dispositivos soportan funcionalidades de Prevención de Intrusión (IPS) que permiten detectar y reaccionar en tiempo real ante potenciales ataques. El componente de IPS permite la aplicación de firmas de ataque predefinidas o *personalizadas*.
4. A esto, se añaden también las funcionalidades de AntiVirus, DLP y análisis de contenido para un control y gestión más granular.
5. Asimismo, proporciona funcionalidades de mejora de rendimiento y reducción de latencia mediante el cacheo estático y dinámico de contenido y la optimización WAN.
6. A través de su integración con el FortiGuard Threat Intelligence Service, permite alimentarse en tiempo real de la inteligencia antiamenazas más reciente de Fortinet, mientras que su integración con FortiSandbox (*Cloud* u *on-premise*) permite abordar la detección de amenazas de día cero (*0-Day*).

2. OBJETO Y ALCANCE

7. En la presente guía se recoge el procedimiento de empleo seguro para las plataformas FortiProxy indicadas en la Tabla 1 que corren la versión FortiProxy 1.0.

Gama Baja	Gama Media	Gama Alta
FortiProxy-400E	FortiProxy-2000E	FortiProxy-4000E

Tabla 1- Modelos Fortiproxy

3. ORGANIZACIÓN DEL DOCUMENTO

8. El presente documento se ha organizado en apartados de acuerdo a distintas fases que componen el ciclo de vida del producto:
 - a) **Apartado 4.** En este apartado se recogen aspectos y recomendaciones a considerar antes de proceder a la instalación del producto.
 - b) **Apartado 5.** En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.
 - c) **Apartado 6.** En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.
 - d) **Apartado 7.** En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.
 - e) **Apartado 8.** En este apartado se muestra un *checklist* con las principales tareas a realizar.
 - f) **Apartado 9.** Este apartado contiene la documentación a la que se ha hecho referencia a lo largo de este documento.
 - g) **Apartado 10.** Este apartado contiene las abreviaturas que se han sido empleadas a lo largo de este documento.

4. FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

9. Durante el proceso de entrega deberán llevarse a cabo una serie de tareas de comprobación, de cara a garantizar que el producto recibido no se ha manipulado indebidamente y se ha afectado su integridad:
 - a) **Información de envío.** Deberá comprobarse la documentación del envío para verificar que concuerda con la orden de compra original, y que el envío ha sido realizado por Fortinet.
 - b) **Embalaje externo.** Deberá inspeccionarse el embalaje y la cinta de embalaje con la marca Fortinet. Se comprobará que la cinta está intacta, que no ha sido cortada ni se ha deteriorado en ningún punto. Así mismo, la caja no deberá presentar cortes ni daños que permitan acceder al dispositivo.
 - c) **Embalaje interno.** Deberá inspeccionarse la bolsa de plástico y el sistema de sellado. La bolsa no deberá presentar cortes ni haber sido extraída. El sistema de sellado deberá estar intacto.
 - d) **Sello de garantía.** En caso de llevarlo, se deberá verificar que el sello de garantía de la unidad está intacto. Se trata de una pequeña etiqueta gris con el logotipo de Fortinet, y normalmente se coloca sobre un tornillo de acceso al chasis. El chasis no se puede abrir sin que este sello sea destruido.
10. En caso de identificarse algún problema durante la inspección, se deberá contactar con Fortinet, al que se le indicará el número de pedido, el número de seguimiento y una descripción del problema.
11. La documentación enviada junto al dispositivo incluye una guía de inicio rápida, junto con un suplemento para el modelo hardware específico. El manual de *FortiProxy Administration Guide* [REF2] proporciona información detallada sobre los procesos de instalación y configuración del dispositivo y de todas sus funciones.

4.2 ENTORNO DE INSTALACIÓN SEGURO

12. El dispositivo deberá instalarse dentro de un Centro de Proceso de Datos (CPD), cuyo acceso estará limitado a un conjunto de personas que posean una autorización expresa.
13. Para ello, la sala en la que se ubica el CPD estará dotada de un sistema de control de acceso que asegure que únicamente personal autorizado puede acceder al dispositivo (incluido fuera del horario laboral).

4.3 REGISTRO DE UNIDAD

14. Se deberá registrar el dispositivo para poder acceder a las diferentes compilaciones del *firmware*, soporte técnico, cobertura de garantía, etc. Será posible registrarse a través de la página web *Fortinet Support Website* (<https://support.fortinet.com/>). Se recomienda que esta labor se realice siempre con la misma cuenta de usuario, de modo que sea posible gestionar la caducidad y renovaciones del mantenimiento y de los servicios de todos los dispositivos de forma centralizada.
15. Para más detalles sobre el proceso de registro, acceder a [Fortinet Support Website Guide\[REF5\]](#):
16. En este enlace se ofrecen diferentes guías, disponibles para su descarga en formato PDF. La primera guía incluye los pasos necesarios para llevar a cabo la creación de una cuenta de soporte. La creación de dicha cuenta es necesaria para llevar a cabo el registro de productos de Fortinet.
17. Los pasos necesarios para llevar a cabo el registro de un producto de Fortinet se explican en la guía "[2.01 Asset Management How to Register a New Product-v5.pdf](#)"
18. En el documento [4.01 Download Center Firmware Images Download-v5.pdf](#) se proporciona información acerca del procedimiento a seguir para llevar a cabo la comprobación de la integridad del firmware/software descargado.
19. En el enlace <https://kb.fortinet.com/kb/documentLink.do?externalID=FD37714> se recomienda la utilización de **herramientas de terceros** para llevar a cabo el cálculo del *checksum* de las imágenes de firmware/software descargadas del centro de soporte de Fortinet. El resultado de dicha operación puede ser comparado con el *checksum* proporcionado en el portal web "**Fortinet Customer Service and Support**". El *checksum* de una imagen se proporciona en el momento de su descarga.
20. A continuación, se introduce un listado con las diferentes guías que se proporcionan en la página web de soporte de Fortinet:
 - a) [1.01 Account Management Create A Support Account-v5.pdf](#)
 - b) [1.02 Account Management Create and Edit a Sub account-v5.pdf](#)
 - c) [1.03 Account Management Recover A Lost Account ID and Password.pdf](#)
 - d) [1.04 Account Management View and Edit a Support Account.pdf](#)
 - e) [2.01 Asset Management How to Register a New Product-v5.pdf](#)
 - f) [2.02 Asset Management Modules and Chassis Registration V1.pdf](#)
 - g) [2.03 Asset Management Add or Renew a Support Contract V1.pdf](#)
 - h) [2.04 Asset Management Virtual Machine \(VM\) License Registration.pdf](#)
 - i) [2.05 Asset Management LENC License Registration.pdf](#)
 - j) [2.06 Asset Management Renew Service On-line.pdf](#)
 - k) [2.07 Asset Management Register a Product after an RMA V1.pdf](#)

- l) [2.08 Asset Management VDOM License Registration V1.pdf](#)
- m) [2.09 Asset Management Premium Support Service RegistrationV1.pdf](#)
- n) [2.10 Asset Management Update Product Description and Partner Info.pdf](#)
- o) [2.11 Asset Management Update the Product Location Address.pdf](#)
- p) [2.12 Asset Management Generating reports from the Support Portal.pdf](#)
- q) [2.13 Asset Management View the details of a Product and Service Entitlement.pdf](#)
- r) [2.14 How to move a contract that has been registered against the wrong Serial Number.pdf](#)
- s) [2.15 License not Updated on GUI V1.pdf](#)
- t) [2.16 How to activate FortiToken Mobile trial V1.pdf](#)
- u) [2.17 FortiClient 6.2.pdf](#)
- v) [2.18 Fortinet Warranty and Contract Start Policy.pdf](#)
- w) [3.01+Assistance+Center Ticket+Creation+Guide.pdf](#)
- x) [4.01 Download Center Firmware Images Download-v5.pdf](#)
- y) [4.02+Download+Center FortiGuard+Service+Updates11.pdf](#)
- z) [4.04+Download+Center Verify+the+Checksum+of+a+Firmware+Image.p
df](#)
- aa) [5.01 How to Enable 2Factor from FortinetOne Portal.pdf](#)

4.4 CONSIDERACIONES PREVIAS

21. A continuación, se indican una serie de recomendaciones y aspectos que se deben tener en cuenta antes de proceder a la instalación y configuración del dispositivo.

4.4.1 MODO DE FUNCIONAMIENTO DEL PROXY

22. Los proxies FortiProxy pueden trabajar en modo enrutador (*NAT/Route Mode*) o en modo transparente (*Transparent Mode*).
23. En modo enrutador el equipo actúa como un dispositivo de nivel 3, encaminando los paquetes entre los diferentes interfaces físicos y lógicos, con la capacidad de hacer NAT (*Network Address Translation*).
24. En modo transparente el dispositivo se comporta como un *bridge* de capa 2, dejando pasar los paquetes en función de las políticas definidas. No tiene direcciones IP en sus interfaces (solamente posee una dirección IP para la gestión y actualización), por lo que puede introducirse en una red sin hacer ninguna modificación. Este modo sirve para realizar escaneos de seguridad sobre el tráfico.

25. Para más información sobre la configuración de los dos modos anteriores consultar *FortiProxy Administration Guide [REF2]*, capítulo “*Transparent and NAT/Route modes*”. Además de esto, para cada funcionalidad en particular se detalla el funcionamiento y configuración en modo transparente.
26. En cuanto al proxy web específicamente, este puede, a su vez, funcionar como proxy web explícito o como proxy web transparente.
27. El FortiProxy, para funcionar como proxy web explícito, puede ser desplegado en cualquier localización de la red. Es necesario configurar los navegadores web para realizar las peticiones de manera explícita a la unidad FortiProxy, ya sea manualmente, por GPOs (Directivas de Grupo) o mediante autoconfiguración a través de ficheros PAC (Proxy Auto-Config). Los ficheros PAC proporcionan configuraciones automáticas de proxy para los proxies web explícitos. FortiProxy también permite el proxy de sesiones FTP en navegadores web.
28. El proxy web recibe sesiones desde un navegador web. FortiProxy actuará como proxy para estas sesiones con el modo web proxy explícito habilitado. El proxy web enruta las sesiones a través de la unidad FortiProxy hacia la interfaz de destino. Antes de que la sesión abandone la interfaz de salida, el proxy web explícito cambia la dirección de origen de los paquetes de sesión, sustituyéndola por la dirección IP de la interfaz de salida o por una IP previamente configurada como SNAT (**en este caso, la dirección IP de origen de los paquetes de la sesión será cambiada por una dirección IP previamente definida**). El proxy web explícito puede ser configurado para que se conserve la dirección IP de origen del cliente.
29. *Proxies* web explícitos y *proxies* FTP pueden operar al mismo tiempo en las mismas o diferentes interfaces de la unidad FortiProxy.
30. Desde la interfaz de línea de comandos (CLI) se puede configurar un proxy web explícito para soportar sesiones SOCKS (el protocolo SOCKS es un protocolo de Internet que permite usar de manera transparente los servicios de *proxies* de red. Es decir, permite llevar a cabo conexiones autorizadas a servidores a través de soluciones de seguridad para la navegación) asociadas a un navegador web.
31. Para más información sobre la configuración del proxy web explícito, consultar *FortiProxy Administration Guide [REF2]*, capítulo “*Web proxy concepts*” y “*Explicit web proxy concepts*”.
32. El proxy web transparente se configura con el FortiProxy en modo transparente, y actúa de proxy para las conexiones de los clientes sin realizar ninguna modificación en la red, ni reconfigurar el navegador o publicar un fichero PAC. Un proxy web transparente puede ser empleado en redes en las que la autenticación basada en direcciones IP no es efectiva, ya que permite la autenticación web basada en el navegador del usuario, y no en su dirección IP.
33. Permite, además, realizar autenticación al tráfico HTTP mediante distintos métodos activos como *Digest (Digest Access Authentication)* o formularios personalizables y también pasivos, como FSSO (Fortinet *Single Sign-On*) o Kerberos. Para más

información, ver la Guía de Administración de FortiProxy, en su capítulo *User&Authentication* [REF2].

34. Por defecto, cuando la unidad FortiProxy se encuentra operando en modo transparente, el proxy web explícito cambia las direcciones IP de origen, sustituyéndolas por la dirección IP empleada por la unidad FortiProxy en su interfaz de gestión. También es posible utilizar la característica Central NAT Table para modificar esta IP por la que se necesite para el servicio. La característica Central NAT Table permite definir reglas para direcciones IP de origen, así como puertos de origen.
35. A continuación, se introducen los comandos de consola necesarios para habilitar Central NAT Table en el dispositivo:

```
Config system settings
    Set central-nat enable
end
```

36. La configuración completa de esta característica se muestra en la Guía de Administración de FortiProxy [REF2], en su capítulo *Central SNAT*.
37. Para más información sobre la configuración del proxy web transparente, consultar *FortiProxy Administration Guide* [REF2], capítulo “*Web proxy concepts*” y “*Transparent web proxy concepts*”.
38. FortiProxy también puede operar como un servicio de caché WCCP (Web Cache Communication Protocol) [REF6]. Este estándar de comunicación redireccionará, generalmente desde un enrutador u otro dispositivo con capacidades WCCP, los paquetes que deben ser inspeccionados por la unidad proxy de forma transparente para los usuarios. Si la consulta existe en caché, lo entregará directamente. En caso contrario, consultará el sitio web para devolver el resultado correspondiente aplicando los perfiles de protección que hayan sido configurados.
39. El servicio de caché WCCP puede ser empleado como un servicio de caché que proporciona balanceo de carga y tolerancia a fallos. Un servidor WCCP recibe peticiones HTTP procedentes de un navegador web, redirigiendo dichas peticiones a uno o más clientes WCCP.
40. Las unidades FortiProxy pueden operar como servidores o como clientes WCCP. Las unidades que operan como servidores WCCP interceptan las sesiones que serán cacheadas. Para interceptar dichas sesiones, el servidor WCCP debe incluir una política en el firewall que acepte dichas sesiones, y el servicio WCCP debe estar habilitado en dicha política. Estos servidores deben contar con una interfaz configurada para mantener comunicaciones WCCP con sus respectivos clientes.
41. Las unidades que operan como clientes usan el puerto 2048/UDP para las comunicaciones WCCP. La configuración de un cliente WCCP se puede llevar a cabo desde el CLI o GUI. A continuación, se describen los pasos a realizar para llevar a cabo la configuración desde el GUI:
 - a) Ir a **Network > Interfaces**.

- b) Seleccionar una interfaz y, a continuación, seleccionar **Edit**.
 - c) Si no hay interfaces en la lista, seleccionar **Create New**.
 - d) Seleccionar **Enable WCCP Protocol** para habilitar WCCP en la interfaz, y seleccionar **OK**.
 - e) Ir a **System > Settings**.
 - f) Seleccionar **Enable** para el WCCP Cache Engine y, a continuación, seleccionar **Apply**.
 - g) Ir a **System > WCCP Settings** y seleccionar **Create New**.
 - h) Configurar los siguientes parámetros: Server ID, Cache ID, Router List, Authentication, Cache Engine Method, Assignment Method.
 - i) Seleccionar **OK** para crear el cliente WCCP.
42. Para más información sobre la configuración del modo WCCP, así como la configuración de clientes WCCP, consultar *FortiProxy Administration Guide* [REF2], capítulo “WCCP”.

4.4.2 ENRUTAMIENTO

43. Los *proxies* FortiProxy soportan enrutamiento estático, tanto IPv4 como IPv6.
44. Es posible añadir diferentes destinos para cada ruta estática, de modo que cuando la ruta primaria no está disponible, los paquetes se encaminan por la siguiente ruta disponible. Para poder detectar la caída de una interfaz, se puede emplear la funcionalidad *link monitor*, que permite monitorizar la ruta de salida mediante el envío de paquetes ICMP, TCP-echo o UDP-echo, entre otros. Si no se recibe respuesta, se considera la ruta caída y comienza a utilizar una ruta alternativa.
45. Cuando el enrutado se hace mediante rutas estáticas, se pueden configurar múltiples rutas para un mismo destino y soportar redundancia entre ellas mediante el mecanismo ECMP (*Equal Cost Multi-path*), de la siguiente manera:
- source-ip-based:** se balancea el tráfico entre las distintas rutas de salida ECMP en función de las direcciones IP origen.
46. Para añadir rutas estáticas para controlar el flujo de tráfico que pasa por la unidad, hay que ir a **Network > Static Routing**. A continuación, hay que seleccionar la opción **Create New > IPv4 Static Route** o **IPv6 Static Route**.
47. Adicionalmente, en el menú de **Static Routing** se ofrecen diferentes opciones, entre ellas la modificación de parámetros de una ruta estática existente, la clonación de una ruta existente, o su eliminación.
48. Para más información sobre la configuración del enrutamiento, consultar *FortiProxy Administration Guide* [REF2], capítulo “Static Routing”.

4.4.3 ALTA DISPONIBILIDAD

49. Es posible configurar un *cluster* para dotar al sistema de redundancia ante fallos. Se puede configurar en modo Activo-Pasivo, en el que sólo el equipo activo procesa el tráfico de red, y es monitorizado por los demás para sustituirle en caso de fallo.
50. Para proteger la integridad del dispositivo, así como las comunicaciones que soporta este, se recomienda considerar siempre el uso de soluciones basadas en *cluster*.
51. Un *cluster* en modo Activo-Pasivo consiste en un equipo primario que procesa todo el tráfico y uno subordinado que está conectado a la red y al equipo primario, pero que no procesa tráfico alguno. No obstante, el nodo secundario puede tener una copia de la tabla de sesiones de los clientes para que, en caso de balanceo, el impacto sea irrelevante, conservando, por ejemplo, el estado de una descarga de un fichero. Esta capacidad se habilita gracias a la opción "Enable Session Pick-up".
52. Para ver la tabla de sesiones a través del CLI, se puede emplear el siguiente comando:

```
#diagnose sys session list
```

53. Para formar el *cluster*, los equipos de FortiProxy utilizan un protocolo específico para la sincronización: FGCP (*Fortigate Cluster Protocol*).
54. El *cluster* puede estar formado por 2 dispositivos. Todos los equipos tienen que tener el mismo hardware y Sistema Operativo. Esta funcionalidad se soporta en modo Enrutador y Transparente.
55. Los miembros del *cluster* se comunican entre ellos a través de un protocolo propietario denominado HA *heartbeat*. Este protocolo se utiliza para:
 - a) Sincronizar la configuración entre los equipos.
 - b) Sincronizar la tabla de sesiones activas.
 - c) Informar a los otros miembros del *cluster* del estado del equipo y sus enlaces.
56. Se recomienda que las interfaces empleadas para la transmisión del tráfico HA *heartbeat*, sean configuradas de modo redundante, es decir, al menos dedicar dos enlaces, y dedicadas para proteger la integridad del *cluster*.
57. FortiProxy permite compartir la cache de los equipos en HA, y que por tanto no sean únicas y aisladas para cada nodo del *cluster*, a través de la herramienta Cache Collaboration. Para más información al respecto, se recomienda consultar el apartado "Cache Collaboration" de la Guía de Administración del producto [REF2].
58. La configuración de alta disponibilidad se realiza desde el interfaz web: **System > HA**. Para más información consultar *FortiOS Handbook* [REF4], capítulo "High Availability".

4.4.4 OPTIMIZACIÓN WAN

59. La optimización o aceleración WAN, posibilita la mejora y el incremento de rendimiento y seguridad en las comunicaciones a través de redes de área extensa, como puede ser el caso de Internet.
60. La tecnología de compresión utilizada es propiedad de Fortinet, con lo que no es compatible con aceleradores de terceros.
61. Las principales funcionalidades aportadas son la optimización de la comunicación, reducción del ancho de banda consumido gracias a la optimización del protocolo de comunicación utilizado, *byte caching*, *web caching*, *SSL offloading* y la posible protección de la comunicación cliente/servidor a través de la red WAN gracias al establecimiento de un túnel seguro, entre otros. Con esto se reducen latencias, se incrementa el rendimiento y se garantiza la privacidad en la comunicación.
62. Dicha tecnología requerirá el soporte de la tecnología de optimización en ambos extremos remotos.
63. La Optimización WAN es transparente para los usuarios. Esto significa que, aunque la Optimización WAN esté habilitada, los clientes serán capaces de conectarse a servidores de la misma forma que si la Optimización WAN estuviera desactivada. Sin embargo, los servidores que reciban paquetes tras la habilitación verán direcciones de origen diferentes, dependiendo de si el Modo Transparente ha sido seleccionado para la Optimización WAN o no.
64. Si el Modo Transparente es seleccionado, se mantendrá la dirección de origen de los paquetes, por lo que parecerá que los servidores reciben tráfico directamente desde los clientes. Si el Modo Transparente no ha sido seleccionado, la dirección de origen de los paquetes será sustituida por defecto, por la IP de la interfaz, o, en caso de configurar SNAT, la IP que haya sido definida.
65. Para llevar a cabo la configuración de perfiles de Optimización WAN, es necesario ir a **WAN Opt. & Cache > Profiles**.
66. A continuación, se describen los pasos necesarios para crear un nuevo perfil de Optimización WAN:
 - a) Desde la lista de perfiles de Optimización WAN, o bien desde la página de edición de perfiles de Optimización, seleccionar **Create New**.
 - b) Introducir la información requerida y, a continuación, seleccionar **OK**.
67. A continuación, se describen los pasos necesarios para modificar un perfil de Optimización WAN:
 - a) Desde la página de edición de perfiles de Optimización, seleccionar el perfil que se desea modificar. Alternativamente, dicho perfil puede ser seleccionado desde el listado de perfiles disponibles, haciendo doble click en el nombre de dicho perfil.
 - b) Editar la información del perfil, y hacer click en **Apply** para guardar los cambios.

68. A continuación, se describen los pasos necesarios para clonar un perfil de Optimización WAN:
- Desde la página de edición de perfiles de Optimización, seleccionar el perfil que se desea clonar.
 - Seleccionar **Clone** desde la barra de herramientas.
 - Introducir un nombre para el perfil en la ventana de diálogo y seleccionar **OK**.
 - Editar el perfil clonado.
69. A continuación, se describen los pasos necesarios para eliminar uno o varios perfiles de Optimización WAN:
- Desde el listado de perfiles disponibles, seleccionar el perfil o perfiles que se desea eliminar.
 - Seleccionar **Delete** desde la barra de tareas.
 - Seleccionar **OK** en la ventana de confirmación.
70. Siempre será recomendable optimizar los recursos mediante técnicas de cache y el cifrado de las comunicaciones, pero se deberá implementar mediante el hardware y los protocolos que indique la política de seguridad a aplicar (CCN- STIC).
71. Para más información sobre la configuración del enrutamiento consultar *FortiProxy Administration Guide [REF2]*, capítulo “WAN Optimization”.

4.4.5 AUTENTICACIÓN

72. A continuación, se indican los principales métodos de autenticación de usuarios o dispositivos, que puede utilizar la unidad FortiProxy.
73. **Autenticación por credenciales.** El método de autenticación más simple es el basado en las cuentas de usuario. Para cada cuenta, se indica el usuario y contraseña (ver apartado 6.3.3 POLÍTICA DE CONTRASEÑAS). Esta autenticación puede ser local, cuando las credenciales se almacenan localmente en la unidad FortiProxy, o puede utilizarse un servidor externo de autenticación.
74. El uso de servidores externos de autenticación es recomendable cuando varias unidades FortiProxy deben autenticar a los mismos usuarios, o cuando una unidad FortiProxy se añade a una red que ya dispone de servidores de autenticación. FortiProxy soporta el uso de FortiAuthenticator, LDAP, RADIUS, TACACS+, Fortinet *Single Sing-On* (FSSO), RADIUS *Single Sing-On* (RSSO), AD, Kerberos o portal cautivo.
75. Cuando se usa un servidor externo de autenticación, FortiProxy envía las credenciales introducidas por el usuario al servidor externo. La contraseña se envía cifrada. La respuesta del servidor indicará si las credenciales son válidas o no.
76. La unidad FortiProxy se deberá configurar para acceder al servidor externo. Esta configuración incluye los parámetros necesarios para autenticar a la unidad

FortiProxy contra el servidor de autenticación. La configuración se realiza a través del interfaz web: *User & Device > RADIUS Servers / LDAP Servers*

/ TACACS+ Servers /Single Sign-On, /Kerberos, etc.

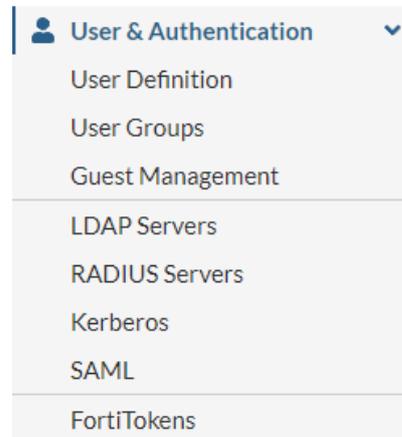


Figura 1 – Menú User & Authentication

77. **Autenticación por certificado.** La unidad FortiProxy puede utilizar certificados X.509 para autenticarse a sí misma (autenticación de servidor), o para autenticar a otros servidores o a usuarios (autenticación de cliente). Los certificados pueden ser auto-firmados (*self-signed*) o pueden ser emitidos por una CA. **Se recomienda la autenticación por certificado emitido por una CA externa de confianza.**
78. **Autenticación SSH por clave pública (*SSH public key authentication*).** Para el establecimiento de conexiones SSH con la unidad FortiProxy, se utilizarán parejas de claves pública-privada, de forma que la clave pública del cliente deberá estar instalada en el servidor y viceversa.
79. **Autenticación por política de seguridad (*Security Policy Authentication*).** Las políticas de seguridad controlan el flujo de tráfico en la navegación.
Opcionalmente, la política puede permitir el acceso cuando el tráfico sea originado únicamente por una dirección IP específica, usuario o grupo de usuarios. Cuando el acceso se controla por usuario o grupo de usuarios, estos deben autenticarse. Esta autenticación de usuarios, se puede hacer a través de: usuarios locales, certificado, RADIUS, TACACS+, LDAP, Guest (usuarios invitados), FSSO (*Fortinet Single Sign On*) o RADIUS SSO.
80. Cuando la autenticación de usuario está habilitada en una política de seguridad, se emplea un “desafío de autenticación” para cualquiera de los siguientes protocolos (dependiendo del protocolo de conexión empleado): HTTP (que puede ser redirigido a HTTPS), HTTPS, FTP, Telnet. Si el protocolo seleccionado es HTTPS, el usuario se puede autenticar empleando un certificado local.
81. **NOTA:** Si bien Telnet se considera un protocolo inseguro, este queda deshabilitado una vez que se habilita la configuración segura del producto. No se recomienda

emplear este protocolo en ningún caso, al tratarse de un protocolo inseguro. Lo mismo ocurre para el protocolo HTTP.

82. Para configurar los parámetros de autenticación del proxy, ir a **User & Device > Proxy Authentication Settings**.

The screenshot displays the 'Proxy Authentication Setting' configuration interface. Key elements include:

- Authentication Timeout:** A text input field containing the value '5'.
- Protocol Support:** Four checked checkboxes for HTTP, HTTPS, FTP, and Telnet.
- Certificate:** A radio button labeled 'Certificate' is selected, with a dropdown menu showing 'Fortinet_Factory'.
- Active Auth Scheme:** An unselected radio button.
- SSO Auth Scheme:** An unselected radio button.
- Captive Portal:** An unselected radio button.
- Redirecting HTTP user authentication to HTTPS:** A selected radio button.
- Captive portal SSL port number:** A text input field containing '7831'.
- Apply:** A blue button at the bottom center.

Figura 2 – Proxy Authentication Settings

83. A continuación, se introducen los comandos necesarios para configurar los parámetros de autenticación desde la consola (CLI):

```
Config authentication setting
  Set active-auth-scheme <string>
  Set sso-auth-scheme <string>
  Set captive-portal <string>
  Set captive-portal-port <integer value from 1 to
65535; default is 0>
end
```

84. Los métodos de autenticación se pueden combinar para lograr un doble factor de autenticación, lo cual es siempre recomendable. Por ejemplo, para la autenticación de usuario combinar el uso de contraseña con la posesión de un certificado, o de un OTP (*One-Time-Password*).
85. **NOTA:** Por motivos de seguridad, se recomienda la autenticación local sobre la autenticación empleando servidores externos de autenticación.
86. Para más información sobre los métodos de autenticación, dirigirse a FortiProxy Administration Guide [REF2], apartado “Proxy Authentication Settings”.

4.4.6 WEB CACHING

87. El cacheo web permite el almacenamiento en memoria caché de objetos, con objeto de acelerar las aplicaciones y los servidores web y reducir el uso de ancho de banda, carga del servidor y latencia percibida a través de la entrega de esos objetos desde la memoria, en vez de realizar cada vez la petición al servidor original (OCS).
88. El almacenamiento en caché de la web implica el almacenamiento de páginas HTML, imágenes, vídeos, respuestas servlets y otros objetos basados en la web para su posterior entrega cuando sean demandados.
89. A través de la funcionalidad de cacheo web colaborativo, los sistemas FortiProxy permiten que múltiples unidades compartan sus objetos cacheados, aumentando así el almacenamiento y evitando duplicidad de objetos.
90. El cacheo web puede ser empleado en cualquier tráfico HTTP/S. Esto incluye tráfico habitual aceptado por una política de seguridad, tráfico asociado a un proxy web explícito, y tráfico de Optimización WAN.
91. Realizar o no el cacheo de este contenido depende de la política que aplique a este tráfico. En caso de desear habilitarlo, sólo habrá que marcar el check “**Web Cache y/o Web Cache For HTTPS Traffic**”, dentro de **Policy&Objects > Policy**, recogidos en la Figura 3 a continuación.

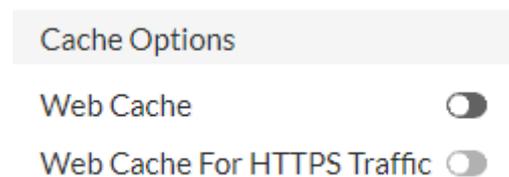


Figura 3 – Cache options dentro de la política

92. Para la activación de la característica de “cache collaboration” es necesario introducir los siguientes comandos:

```
config wanopt cache-service
set collaboration enable
set device-id "fch-1"
config dst-peer
edit "peer-id"
set ip xxx.xxx.xxx.xxx
next
end
end
```

93. Se configurarán tantos “peer-id” como nodos haya dentro del clúster, siendo el valor de esta variable el “device-id” de cada miembro. Todos ellos tienen que ser diferentes. Asimismo, se recomienda numerar los nodos correlativamente con una raíz común en el nombre (fch-1, fch-2, ..., fch-n).

4.4.7 SERVICIO DE ANÁLISIS DE CONTENIDO

94. Los sistemas FortiProxy permiten el análisis del contenido de las webs en tiempo real para la detección de contenido adulto. Cuando contenido de este tipo es detectado, este puede ser bloqueado o reportado.
95. En general, este procedimiento es similar al que sigue el escaneo de un antivirus HTTP. Cuando un cliente HTTP solicita una imagen, se determina el tipo de imagen basándose en la cabecera HTTP *content-type*. La imagen es escaneada antes de ser enviada al cliente. Si la imagen no respeta los criterios establecidos, la imagen solicitada es bloqueada, y el cliente recibe una imagen de reemplazo.
96. Para emplear el servicio de análisis de contenido, es necesario crear al menos un perfil, que debe ser adjuntado a una política. Los perfiles de análisis de contenido se configuran en **Security Profiles > Content Analysis**.

Block Strictness Level				
Alcohol	<input checked="" type="checkbox"/> Allow	<input type="checkbox"/> Deny	<input type="checkbox"/> Monitor	30
Drugs	<input checked="" type="checkbox"/> Allow	<input type="checkbox"/> Deny	<input type="checkbox"/> Monitor	30
Extremism	<input checked="" type="checkbox"/> Allow	<input type="checkbox"/> Deny	<input type="checkbox"/> Monitor	30
Gambling	<input checked="" type="checkbox"/> Allow	<input type="checkbox"/> Deny	<input type="checkbox"/> Monitor	30
Gore	<input checked="" type="checkbox"/> Allow	<input type="checkbox"/> Deny	<input type="checkbox"/> Monitor	30
Porn	<input checked="" type="checkbox"/> Allow	<input type="checkbox"/> Deny	<input type="checkbox"/> Monitor	30
Swim Underwear	<input checked="" type="checkbox"/> Allow	<input type="checkbox"/> Deny	<input type="checkbox"/> Monitor	30
Weapons	<input checked="" type="checkbox"/> Allow	<input type="checkbox"/> Deny	<input type="checkbox"/> Monitor	30

Figura 4 – Perfil de configuración de Content Analysis

97. Para la configuración del perfil, se configurará su nombre y los distintos parámetros de reemplazo. Por último, se ajustarán los umbrales de reconocimiento de cada

categoría en base al estándar de cumplimiento. Se recomienda una primera aproximación seleccionando la acción “Monitor” y analizando los *logs* recibidos, para más tarde pasar a la aplicación de la acción “Deny” con los umbrales más precisos.

5. FASE DE INSTALACIÓN

5.1 PRIMER ACCESO AL DISPOSITIVO

98. Para acceder al dispositivo por primera vez, se conectará el equipo del administrador al puerto de consola del dispositivo y configurará una de las interfaces del dispositivo con una IP estática, ya que el equipo por defecto no tiene IPs asignadas a sus interfaces, excepto en la interfaz/puerto 1, que viene configurada para obtener IP por DHCP. Una vez establecida dicha IP y los permisos de acceso (HTTPS, SSH, PING, etc.) se podrá acceder indicando el usuario por defecto *admin* y sin contraseña.
99. Durante la fase de instalación, el dispositivo no deberá estar conectado a Internet, y preferiblemente estará únicamente conectado al equipo del configurador. Esto es debido a que los valores establecidos por defecto son conocidos y considerados inseguros (incluido el usuario/contraseña), pudiendo comprometer el dispositivo por un atacante.

5.2 INSTALACIÓN DEL FIRMANTE

5.2.1 HABILITACIÓN MODO FIPS

100. El primer paso en la instalación del dispositivo es la descarga e instalación del *firmware*.
101. Se recomienda la instalación de la versión segura de *Firmware*, que es aquella que ha sido evaluada y dispone de la certificación *Common Criteria*: FortiProxy v1.0. Para ello, los pasos a seguir serán los siguientes:
 - a) Primero dirigirse a la página web de soporte (<https://support.fortinet.com>) y acceder con las credenciales obtenidas previamente durante el proceso de registro de la unidad.
 - b) Ir a la página del *firmware*, seleccionar el *firmware* certificado **FortiProxy 1.0.7 FIPS-CC** para el modelo hardware del dispositivo. Descargar el fichero de *firmware* en el equipo que se usará para la instalación y anotar (se encuentra disponible en la misma página, junto al enlace de descarga) el valor del *hash* de comprobación disponible en formato SHA- 512.
 - c) Verificar la integridad del fichero de firmware descargado. Para ello, se calculará el SHA-512 del fichero a través de alguna herramienta apropiada (por ejemplo, **OpenSSL**), y se comparará con el valor del *hash* mostrado en la página de descarga.
 - d) Antes de instalar el nuevo firmware es recomendable obtener la versión instalada en el dispositivo para poder dar marcha atrás en caso de que haya algún problema con la nueva versión. Desde el equipo de administración conectado a consola, y usando el interfaz web: **Dashboard**

> **Main** > **System Information** > **Firmware** o en **System** > **Firmware** > **Current version**

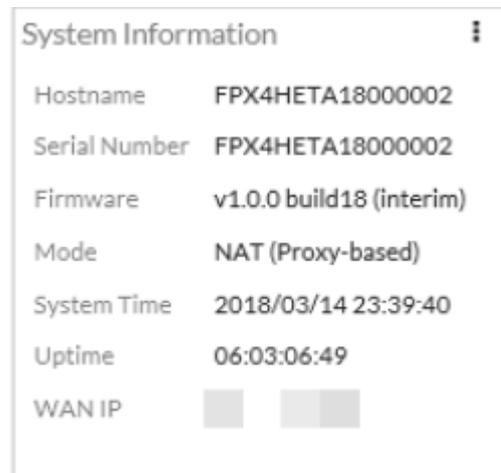


Figura 5 – Widget de System Information dentro del dashboard principal

102. Para la instalación del nuevo firmware, usar la opción “Upload Firmware” en **System** > **Firmware**, seleccionando el fichero de firmware a instalar. La unidad FortiProxy carga el archivo de firmware, actualiza a la nueva versión, se reinicia y muestra el inicio de sesión de FortiProxy. Este proceso toma unos pocos minutos. A continuación, se enumeran los pasos necesarios para subir una nueva imagen de firmware actualizado, y llevar a cabo su instalación.

- a) Ir a **System** > **Firmware** y seleccionar **Upload Firmware**.
- b) Seleccionar el fichero de imagen en el equipo y pulsar **Open**.
- c) Seleccionar **Backup Config and Upgrade**. El sistema se reiniciará.

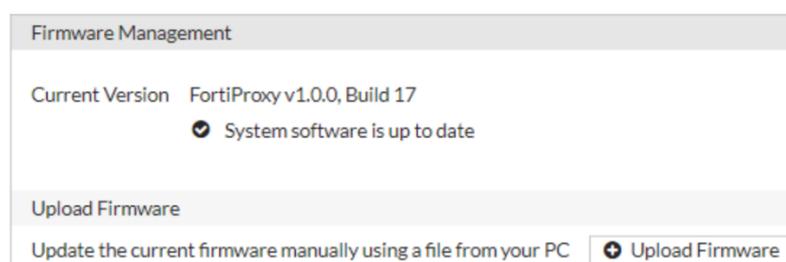


Figura 6 – Menú System > Firmware

103. Finalmente, comprobar que la versión de firmware instalada es la correcta (ver Figura 6). Indicar, que deberá mostrarse una de las build que corresponden a la versión certificada CC, y que es la **v100-build0066 (versión 1.0.7)**.

104. Esta comprobación se puede realizar desde **Dashboard** > **Main** > **System Information** > **Firmware** o en **System** > **Firmware** > **Current version**. También se puede abrir una ventana de la consola del equipo pulsando en el símbolo >_ que se encuentra en la parte superior derecha. En dicha consola se puede ejecutar el

comando “*get system status*”. En la documentación *FortiProxy Administration Guide* [REF2], en el capítulo “Updating firmware” se proporciona mayor detalle y otros métodos para la instalación del firmware.

5.3 ACCESO A BIOS

105. Solo es posible acceder a la BIOS desde la consola del equipo, interrumpiendo el proceso de arranque (pulsando cualquier tecla). Desde la BIOS es posible: ver información del sistema, formatear el dispositivo, cargar un *firmware* y recargar el *backup* de un *firmware* (ver Figura 7).

```
Initializing boot device...
Initializing MAC... nplite#0
Please wait for OS to boot, or press any key to display configuration menu.

[C]: Configure TFTP parameters.
[R]: Review TFTP parameters.
[T]: Initiate TFTP firmware transfer.
[F]: Format boot device.
[I]: System information.
[B]: Boot with backup firmware and set as default.
[Q]: Quit menu and continue to boot.
[H]: Display this list of options.

Enter C,R,T,F,I,B,Q, or H:
```

Figura 7 – Menú de arranque para acceder a BIOS

6. FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

106. El dispositivo debe operar en lo que se denomina **modo de operación seguro**. Al habilitarse este modo, se borrarán todas las configuraciones existentes y se establecerán una serie de parámetros de configuración fijos, que cumplen con un nivel base de seguridad. Entre ellos, se encuentran la complejidad de contraseñas, el cifrado utilizado y otros parámetros que pueden ser analizados en la documentación de *Common Criteria* [REF1]
107. La habilitación del modo de operación seguro **solo se puede llevar a cabo desde consola**. Si el modelo hardware requiere el Fortinet Entropy Token, este debe haberse insertado en el puerto USB correspondiente del dispositivo (tipo USB-A). Al habilitar el modo de operación seguro, se debe habilitar también el uso del *token* de entropía.
108. El RBG (*Random Bit Generator*) del dispositivo se alimenta desde el *token* de entropía durante el proceso de arranque, y luego se realimenta periódicamente. El período de realimentación (*reseed period*) por defecto es una vez cada 24 horas (1440 minutos).
109. Se recomienda configurar un periodo de realimentación de 60 minutos a través del parámetro **self-test-period**.
110. Los comandos para habilitar el modo de operación seguro y la configuración del *token* de entropía son los siguientes:

```
Config system fips-cc
    Set status enable
    Set entropy-token enable
end
```

111. Posteriormente a la habilitación del modo de operación seguro, el dispositivo solicitará introducir la nueva contraseña del administrador mostrando el siguiente mensaje **“Please enter administrator password”**, esta contraseña debe tener una longitud mínima de 8 caracteres, contener letras y números y, al menos, un carácter especial. No obstante, por motivos de seguridad, se recomienda emplear siempre una longitud mínima de 12 caracteres para la contraseña.
112. Una vez introducida la contraseña por segunda vez, aparecerá el mensaje **“Warning: most configuration will be lost, do you want to continue? (y/n)”**, que se deberá responder introduciendo: **y**.
113. Tras esto, la unidad se reiniciará y comenzará a funcionar con el modo de operación seguro activado. Comprobar que este modo ha sido correctamente activado a través del comando:

```
Get system status
```

FIPS-CC mode: enable

114. Indicar que en el caso de que el dispositivo se encuentre configurado en el modo de operación seguro con el *token* de entropía habilitado, si el *token* no se encuentra conectado en el momento de arranque del dispositivo, se mostrará un mensaje en la consola y el proceso de arranque se parará hasta que el *token* sea insertado. El mensaje mostrado será: ***Please insert entropy-token to complete RBG seeding.***

115. Tras activar el modo de operación seguro:

- a) Todos los interfaces de red están desactivados (*down*) y no tienen dirección IP asignada. Es necesario, por lo tanto, configurar los interfaces (ver apartados siguientes).
- b) No está configurada ninguna dirección DNS.
- c) No está configurada ninguna ruta por defecto.
- d) Hay parámetros, funciones y/o servicios del dispositivo que se encontrarán deshabilitados y no podrán ser habilitados:
 - Auto - instalación a través de USB.
 - Servidor local TFTP de la unidad FortiProxy.
 - Comando **fnsysctl**, que proporciona acceso al Sistema Operativo subyacente.
 - Reportes de ataques de virus al servicio FortiGuard FDS (*FortiGuard Distribution Service*).
 - Accesos empleando los protocolos SSH 1.0, TLS 1.1, Telnet y HTTP.

6.2 CERTIFICADOS

116. Se recomienda el uso de certificados en la unidad FortiProxy, para la autenticación en las conexiones HTTPS de administradores, para inspección SSL y para autenticación de usuarios.

117. La unidad FortiProxy utiliza por defecto certificados auto firmados (*self-signed*), pero se recomienda el uso de certificados X.509 emitidos por una CA de confianza. Para ello, la unidad FortiProxy permite generar un CSR (*Certificate Signing Request*) desde el interfaz web: **System > Certificates > Generate**. Es necesario crear el CSR, tanto si se trabaja con certificados autofirmados como si se trabaja con certificados emitidos por una CA de confianza.

Generate Certificate Signing Request

Certificate Name

Subject Information

ID Type **Host IP** Domain Name E-Mail

IP

Optional Information

Organization Unit

Organization

Locality(City)

State / Province

Country / Region

E-Mail

Subject Alternative Name

Password for private key

Key Type **RSA** Elliptic Curve

Key Size

Enrollment Method **File Based** Online SCEP

Figura 8 – Generación CSR en FortiProxy

118. Cuando se genera un CSR, se crea un par de claves (clave pública/clave privada) en la unidad FortiProxy. La petición generada incluye la clave pública del dispositivo, e información como la dirección IP pública de la unidad, el nombre del dominio, o una dirección de correo electrónico. La clave privada permanece en todo momento en la unidad.
119. Una vez que la petición es enviada a la CA de confianza, esta verifica la información y registra la información en un certificado digital que contiene un número de serie, una fecha de expiración, y la clave pública de la CA. A continuación, la CA firma el certificado, tras lo cual puede ser instalado en el dispositivo FortiProxy.
120. Para configurar la autenticación por certificados, será necesario importar los certificados raíz de la CA emisora de los certificados cliente (*root CA certificate*), así como las CRL (*Certificate Revocation List*) de dichas CA. Esto se llevará a cabo desde la interfaz web: **System > Certificates > Import > CA Certificates**, o **System > Certificates > Import > CRL**.

121. A continuación, se enumeran los pasos necesarios para la generación de un CSR.

- a) Desde la página **Certificates**, seleccionar **Generate**.
- b) Se abre la página de generación de Certificate Signing Request.
- c) Introducir la información necesaria.
- d) Seleccionar **OK** para generar el CSR.

122. Los certificados que se instalen en la unidad FortiProxy y en los clientes, deben utilizar claves RSA o ECDSA (*Key Type*) de longitud (*Key Size*), al menos, 3072 bits para RSA, y curvas p256 para ECDSA. Esto permitirá el cumplimiento de los requisitos establecidos en la guía CCN-STIC-807 [REF3] sobre el uso de algoritmos y funciones criptográficas en sistemas de nivel Alto del ENS.

123. **NOTA:** Se recomienda el uso de ECDSA sobre RSA. La Figura 8 muestra la pantalla de creación de Solicitudes de Creación de Certificados. En dicha imagen puede verse como se da la opción de emplear claves RSA (dicha opción ofrece una longitud de 4096, siendo esta longitud considerada segura) o *Elliptic Curve* (ECDSA).

124. En *FortiProxy Administration Guide* [REF2], capítulo “*Certificates*” y capítulo “*Proxy authentication settings*” se puede consultar más información sobre el uso de certificados.

6.3 ADMINISTRACIÓN DEL DISPOSITIVO

125. La administración se configurará de acuerdo a los principios de mínima funcionalidad y mínimo privilegio, es decir, se procurará que los usuarios administradores sean los mínimos posibles y que el conjunto de usuarios administradores en general, no disponga de más privilegios de los que necesite.

126. La administración segura de la unidad FortiProxy se realizará accediendo localmente al dispositivo, bien a través del puerto consola (acceso CLI, utilizando un emulador de terminal en el PC de gestión), bien a través de una conexión directa del PC de gestión a uno de los puertos de red (RJ-45) del dispositivo, lo cual permitirá acceder a través del interfaz web de gestión (*web-based manager*, empleando el protocolo HTTPS), o a través de CLI (utilizando SSH, o utilizando el *widget* CLI que proporciona el interfaz web). En caso de acceder a través de un interfaz de red, deberá habilitarse ese acceso desde consola (CLI):

```
Config system interface
    Edit <interfaz>
        Set allowaccess https ssh
    end
```

127. **No se recomienda la administración remota, salvo que sea estrictamente necesario.** En el modo de operación seguro, la administración remota está deshabilitada por defecto, así como los protocolos HTTP y Telnet. En caso de ser necesario, se habilitará el acceso remoto a uno de los interfaces de gestión, siempre

a través de un protocolo seguro (HTTPS o SSHv2) con los comandos indicados anteriormente.

128. Se puede consultar más información sobre la configuración de administración del dispositivo en *FortiProxy Administration Guide [REF2]*, capítulo “*System Administration*”.

6.3.1 ADMINISTRACIÓN HTTPS (GUI)

129. Las conexiones de administración por HTTPS utilizan un certificado para la autenticación de servidor, que deberá estar instalado en la unidad FortiProxy. Este certificado, por defecto, es auto firmado (*self-signed*). Se recomienda la instalación de un certificado X.509 emitido por una CA de confianza.

130. **Se recomienda configurar la autenticación de cliente por certificado**, lo que añadirá un segundo factor de autenticación, ya que la unidad FortiProxy procesará el certificado de cliente después de que el administrador introduzca su usuario y contraseña.

131. Para habilitar la autenticación de cliente por certificado se deberá:

- a) Obtener un certificado personal para el administrador, firmado por una CA, e instalarlo en el navegador del equipo de administración.
- b) Instalar el certificado raíz de la CA emisora (Root CA certificate) y la CRL (Certificate Revocation List) en la unidad FortiProxy, desde el interfaz web: **System > Certificates > Import > CA Certificates, System > Certificates > Import > CRL.**

The screenshot shows the 'Import CRL' configuration page in the FortiProxy GUI. It features three main sections for import methods: HTTP, LDAP, and SCEP. The 'Import Method' is currently set to 'Online Updating'. The 'HTTP' section has a toggle switch turned on and a text input field for the 'URL of the HTTP server'. The 'LDAP' section has a toggle switch turned on and three input fields: 'LDAP Server' (a dropdown menu), 'Username', and 'Password' (with a visibility icon). The 'SCEP' section has a toggle switch turned on, a 'Certificate' dropdown menu set to 'Fortinet_CA_SSL', and a text input field for the 'URL of the SCEP server'.

Figura 9 – Menú de importación de CRLs

132. Añadir la cuenta de usuario PKI al grupo de usuarios del FortiProxy dedicado a los administradores con autenticación PKI.

```

Config system admin
    Edit <nombre_administrador>
    Set peer-auth enable
    Set peer-group <grupo_PKI>
end

```

133. En la configuración de la cuenta del administrador, seleccionar **Use public key infrastructure(PKI) group** como tipo de cuenta y seleccionar **PKI Group** como grupo de usuarios, aquel al que pertenece el administrador.

The screenshot shows a configuration window for a user. The 'User Name' field contains 'ken.felix@socpuppets.com'. The 'Type' dropdown menu is open, showing options: 'Local User', 'Match a user on a remote server group', 'Match all users in a remote server group', and 'Use public key infrastructure (PKI) group' (which is highlighted in green). Below this, the 'Comments' field is empty with a character count of 0/255. The 'PKI Group' dropdown is set to 'pki'. The 'Email Address' field is empty. At the bottom, there are two toggle switches: 'SMS' (disabled) and 'Restrict login to trusted hosts' (disabled). 'OK' and 'Cancel' buttons are at the bottom right.

Figura 10 – PKI Groups

134. También se puede forzar a que el administrador tenga que proporcionar su certificado personal para administrar el equipo. Si está deshabilitado, los administradores pueden iniciar sesión con un certificado o una contraseña. Para forzar el uso de certificados es posible utilizar este comando:

```

Config system global
    Set admin-https-pki-required enable
end

```

135. La unidad FortiProxy soporta el uso de varias versiones de TLS. **Deberá estar configurada para que haga uso de, como mínimo, la versión TLSv1.2, dado que versiones inferiores se consideran inseguras:**

```

Config system global
    Set admin-https-ssl-versions tlsv1-2
end

```

136. Para más información acerca del uso del interfaz web para la administración, consultar *FortiProxy Administration Guide* [REF2].

6.3.2 CONFIGURACIÓN DE SSH

137. Para la administración CLI a través de SSHv2, se recomienda configurar la autenticación mutua (cliente – unidad FortiProxy), a través de claves públicas.

138. Para ello, se debe generar en el PC usado para la administración SSH, una pareja de claves pública – privada, con una longitud mínima de 3072 bits. La clave pública generada debe ser importada a la unidad FortiProxy a través de los comandos:

```
Config system admin
    Edit admin
        Set ssh-public-key1 <string>
    end
```

139. <string> debe ser la clave pública del cliente. Esta clave debe ser “ssh-dsa” o “ssh-rsa” en función del algoritmo utilizado para la generación de las claves. **Deberán utilizarse claves DSA o RSA de, al menos, 3072 bits de longitud**, con objeto de cumplir los requisitos establecidos en la guía CCN-STIC-807 [REF3] para el uso de algoritmos y funciones criptográficas en Nivel Alto del ENS.

140. Se recomienda, también, especificar el *timeout* máximo para autenticación (*login grace time*, este parámetro hace referencia al tiempo máximo permitido entre el establecimiento de la conexión, y el inicio del proceso de autenticación, por ejemplo, introduciendo las credenciales de usuario), y deshabilitar la versión 1 del protocolo SSH:

```
Config system global
    set admin-ssh-grace-time
    <number_of_seconds>
    set admin-ssh-v1 disable
end
```

6.3.3 POLÍTICA DE CONTRASEÑAS

141. La autenticación por contraseña es un método efectivo únicamente si la contraseña es suficientemente robusta y se cambia periódicamente. Por defecto, la unidad FortiProxy requiere únicamente que las contraseñas sean de, al menos, 8 caracteres de longitud, aunque se permiten hasta 128. Debe establecerse una política de contraseñas que obligue a contraseñas más robustas en cuanto a longitud y complejidad. Se recomienda una longitud mínima de 12 caracteres para las contraseñas.

142. Para especificar la política de contraseñas desde el interfaz web de gestión:

System > Settings > Password Policy.

Password Policy	
Password scope ⓘ	Off Admin IPsec Both
Minimum length	8
Minimum number of new characters	0
Character requirements	<input checked="" type="checkbox"/>
Upper case	0
Lower case	0
Numbers (0-9)	0
Special ⓘ	0
Allow password reuse	<input checked="" type="checkbox"/>
Password expiration	<input checked="" type="checkbox"/> 90 Days

Figura 11 – Política de complejidad de contraseñas en FortiProxy

143. Es necesario especificar una política de contraseñas para la autenticación de administradores, con los siguientes requisitos mínimos (estos valores se configuran automáticamente al entrar en modo FIPS):

- a) Longitud de la contraseña: el producto permite establecer una longitud mínima de 8 caracteres. No obstante, por motivos de seguridad se recomienda configurar una longitud mínima de contraseña de 12 caracteres.
- b) Complejidad:
 - Uno o más caracteres en minúscula.
 - Uno o más caracteres en mayúscula.
 - Uno o más números.
 - Uno o más caracteres especiales.
- c) En el cambio de contraseña, no debe permitirse la reutilización de, al menos, las 5 contraseñas anteriores (este valor se configura a 4 automáticamente al entrar en modo FIPS).

```
Config system password-policy
  Set status enable
  Set reuse-password disable
  Set password-history 5
end
```

- d) El cambio de contraseña debe realizarse cada cierto tiempo. Esto puede ser forzado desde FortiProxy en **System > Settings > Password Policy > Password Expiration**. Se recomienda forzar el cambio de contraseña cada 60 días. Por defecto, el período establecido es de 90 días (este último valor se configura automáticamente al entrar en modo FIPS).
- e) Desde el cambio de contraseña, se recomienda establecer un período de 7 días antes de que esta contraseña pueda ser cambiada de nuevo.
- f) Algunas buenas prácticas en la selección de la contraseña son: evitar palabras de diccionario, secuencias numéricas, secuencias de caracteres seguidos en el teclado, evitar añadir números al final de la palabra o números al final de la contraseña anterior, caracteres repetidos, información personal, etc.

144. Se puede consultar más información sobre la configuración de la política de contraseñas en *FortiProxy Administration Guide* [REF2], capítulo “*System Settings*”.

6.3.4 PARÁMETROS DE SESIÓN

145. A continuación, se indican una serie de parámetros de sesión que será necesario configurar en las conexiones de los administradores a la unidad FortiProxy:

- a) **Timeout de autenticación**, que es el tiempo que permanece el usuario autenticado en la sesión, transcurrido el cual, el usuario debe volver a autenticarse. Esto evita que, en caso de que la conexión del usuario legítimo sea suplantada (*spoofed*), pueda ser utilizada de forma malintencionada durante largo periodo de tiempo.

Esta configuración se realiza desde el interfaz web: **User & Device > Proxy Authentication Setting > Authentication Timeout**.

NOTA: El tiempo por defecto es de 5 minutos, y se recomienda no ampliar este valor en el Modo Seguro.

- b) **Sesiones concurrentes de un administrador**, de forma que solo haya una sesión activa:

```
Config system global
    set admin-concurrent disable
end
```

- c) Número de administradores que pueden acceder simultáneamente a la unidad FortiProxy (*admin-login-max*):

```
Config system global
    set admin-login-max <number>
end
```

- d) **Timeout de inactividad para las conexiones de consola (admin-console-timeout) y para las conexiones remotas (admin-timeout).** Transcurrido este tiempo con la sesión inactiva, se producirá la desconexión automática. Al igual que el admin-timeout (tiempo de inactividad para sesiones de administración) del interfaz gráfico, el valor por defecto son 300 segundos de esta forma, se evita que las sesiones de administración queden abiertas tras finalizar un trabajo. Este valor, aunque no es recomendable, se puede obviar configurándolo a 0, o a su valor mínimo, que es de 15 segundos. Se recomienda dejar el valor por defecto de 300 segundos.

```
Config system global
    set admin-console-timeout <sgs>
end
```

- e) **Número máximo de intentos fallidos de autenticación (admin-lockout-threshold), y un tiempo de espera tras superar dicho umbral (admin-lockout-duration),** evitando de esta manera ataques de fuerza bruta. Se recomienda establecer el valor de número máximo de intentos fallidos de autenticación a **3 intentos**, y el tiempo de espera tras superar dicho umbral a **5 minutos**.

Esta configuración se puede realizar a través de los siguientes comandos:

```
config system global
    set admin-concurrent disable
    set admin-console-timeout 300
    set admin-lockout-duration 300
    set admin-lockout-threshold 3
    set admin-login-max 1
    set admin-timeout 300
end
```

146. Es importante destacar que, en las sesiones CLI, cuando el administrador hace log-out o el tiempo de inactividad de sesión se cumple, el dispositivo FortiProxy envía 300 caracteres de retorno de carro para limpiar la pantalla. Si el buffer del terminal que se está utilizando es muy grande, puede que no se borre toda la información de la sesión.

6.3.5 USUARIO “ADMIN”

147. El usuario “admin” es el usuario creado por defecto, por lo que debe limitarse su uso a la gestión local y siempre desde dispositivos seguros, y emplear para la administración, usuarios personalizados y con el perfil estrictamente necesario.

148. Es imprescindible establecer la nueva contraseña robusta del usuario “admin”, y restringir las direcciones IP origen desde las que puede acceder a la unidad FortiProxy.

```
config system admin
  edit "admin"
    set trusthost1 <direccionIP>
    < mascara>
    set password <contraseña>
    set accprofile super_admin
    set comments <comentario>
  next
end
```

149. Es recomendable, también, establecer un segundo factor de autenticación. Por ejemplo, a través de un dispositivo OTP (*One Time Password*). Fortinet proporciona dispositivos OTP conocidos como FortiToken.

```
config system admin
  edit "admin"
    set two-factor fortitoken
    set fortitoken <NumerodeSerie>
  next
end
```

150. También es posible emplear otros mecanismos para la autenticación de dos factores mediante el envío de SMS o correo electrónico.

151. Se recomienda la utilización de autenticación de más de un factor para el usuario “admin”. El método de autenticación vendrá reflejado en la política de seguridad correspondiente. Se utilizarán usuarios nominales únicos para cada administrador y durante el tiempo estrictamente necesario.

6.3.6 MENSAJE DE AVISO Y CONSENTIMIENTO

152. Antes del establecimiento de una sesión de administración, el sistema deberá mostrar un mensaje de aviso sobre las restricciones de uso de la conexión (*pre-login disclaimer banner*). Los administradores deberán aceptar el mensaje, previo al establecimiento de la conexión. En dicho mensaje, no se facilitará información del sistema que pueda identificarlo o caracterizarlo ante un atacante.

153. La habilitación de este *banner* se hará a través de la consola de comandos CLI utilizando una cuenta con permisos de “super_admin”, ya sea la cuenta de administrador por defecto (admin) o una creada previamente. Se deberán introducir los siguientes comandos:

```
config system admin
    set pre-login-banner enable
end
```

154. Al habilitar el *banner* mencionado arriba, se habilitará también otro, que se mostrará inmediatamente después del inicio de la sesión de administración. En caso de querer deshabilitar este *banner*, se deberán introducir los siguientes comandos:

```
config system admin
    set post-login-banner disable
end
```

155. Cada *banner* es un mensaje por defecto que podrá personalizarse a través del interfaz web en **System > Replacement Messages**, o a través del comando "***config system replacemsg***".

6.4 USUARIO MAINTAINER

156. Los dispositivos FortiProxy disponen de un usuario *Maintainer* que, a través del puerto de consola, permite tener acceso al dispositivo en el caso de no recordar las credenciales de administración. Este usuario no aparece en la consola de administración web.

157. Debe impedirse el acceso local a la configuración del dispositivo en el caso de no conocer las credenciales de administración, para lo cual, el usuario *Maintainer* deberá deshabilitarse.

158. Para ello, ejecutar los siguientes comandos:

```
config system admin
    set admin-maintainer disable
end
```

159. De este modo, en caso de necesidad de recuperar el equipo, se debe interrumpir el arranque de éste y reinstalar un firmware nuevo con una configuración por defecto.

6.5 CONFIGURACIÓN DE INTERFACES

160. **Los interfaces no utilizados del dispositivo deberán deshabilitarse.** De este modo se minimizan los riesgos de exposición a ataques en interfaces que no se utilizan, así como problemas derivados de errores al conectar los cables a puertos incorrectos del equipo.

161. Para ello, se ejecutará el comando **set status down** en el interfaz en cuestión:

```
config system interface
    edit "<interfaz>"
```

```
set status down
```

```
next
```

162. Desde la interfaz web, es posible deshabilitar los interfaces que estén habilitados en **Network > Interfaces**. Se edita el interfaz y se marca como “*Disabled*” la sección “*Status*”, que se encuentra al final de las opciones.
163. Además, se recomienda introducir una etiqueta que identifique el uso para el que está destinado cada interfaz. De este modo, se minimizan los riesgos de error en la configuración, modificaciones, etc.
164. Para ello, se ejecutará el comando **set alias** en el interfaz en cuestión. Por ejemplo, para identificar que el interfaz es de acceso a internet:

```
config system interface
```

```
edit "<interfaz>"
```

```
o set alias “internet”
```

```
next
```

165. Desde la interfaz web se pueden añadir alias en **Network > Interfaces**. Editando el interfaz se encuentra, como primera opción, la caja de texto en la que introducir esta descripción, llamada *Alias*.
166. Respecto a los servicios disponibles por puerto o interfaz, existen algunos que, por su naturaleza, no deben estar activos nunca. Otros, sólo en caso de que sean imprescindibles. En cualquier caso, siempre hay que seguir el principio de mínima funcionalidad de modo que sólo se encuentren activos únicamente aquellos servicios necesarios.
167. A continuación, se realizan una serie de indicaciones relativas a servicios y protocolos:
- Es preferible la asignación estática de direcciones IP, por lo que se recomienda deshabilitar el protocolo DHCP si no hay razones de escalabilidad que lo justifiquen (**set dhcp-relay-service disable**). La obtención de direccionamiento de forma dinámica, posibilita la opción de recibir estas IPs de un servidor no autorizado o simplemente erróneo, comprometiendo la seguridad y el servicio.
 - Se deberá deshabilitar cualquier mecanismo de detección de fallo de un interfaz, para evitar que dicho mecanismo pueda ser manipulado por un atacante, y crear con ello una denegación de servicio (**set fail-detect disable**). Un atacante podría enviar paquetes especialmente formados para simular un problema en los interfaces, y poner el servicio en una situación de compromiso.
 - Siempre que sea posible, se implementará algún mecanismo de autenticación de red mediante portal cautivo (**set security-mode <captive-portal>**).

168. Los comandos para realizar estas acciones, son los siguientes (consultar más información en *FortiProxy CLI Reference* [REF3]).

```
config system interface
    edit "<interfaz>"
        set dhcp-relay-service disable
        set fail-detect disable
        set security-mode <captive>
    next
```

6.6 CONFIGURACIÓN DE SERVICIOS DEL DISPOSITIVO

169. En base al principio de mínima funcionalidad, **deberán deshabilitarse todos los servicios que no sean imprescindibles**. Muchos de los servicios están deshabilitados por defecto, pero siempre es recomendable comprobar su estado desde el CLI.

170. A continuación, se realizan una serie de indicaciones consideradas como un conjunto de buenas prácticas, relativas a servicios y protocolos:

- a) El número de entradas ARP máximo configurado por defecto es 131.072. Si no es suficiente se deberá ajustar al valor adecuado a la red.
- b) No deberá extenderse el periodo de autenticación de la sesión para evitar el tiempo de timeout (variables *admin-timeout* y *admin-console-timeout*, mencionadas en apartados anteriores). Esto es, no deberá permitirse que una sesión permanezca activa durante mucho tiempo, ya esté inactiva o no, para evitar posibles brechas de seguridad. Este punto se aplica tanto para conexiones locales como para conexiones remotas.
- c) No se deberá permitir que pase tráfico sin escanear en situaciones de consumo excesivo de memoria.
- d) Se deberá habilitar la comprobación de los paquetes de error ICMP.
- e) Deberá habilitarse el *timestamp* de los mensajes de log. Es decir, los mensajes de log deberán incluir una marca de tiempo.
- f) Por último, se habilitará, mediante el motor IPS, la detección de ficheros con formato Hibun. Este protocolo de cifrado está muy extendido para el intercambio de ficheros (sobre todo ficheros multimedia) sensibles de ser exfiltrados de la organización.

171. Los comandos para realizar estas acciones son los siguientes (consultar más información en *FortiProxy CLI Reference* [REF3]).

```
config system global
    set arp-max-entry 131072
    set auth-keepalive disable
```

```
set av-failopen off
set av-failopen-session enable
set check-reset-range strict
set fds-statistics enable
set fgd-alert-subscription advisory
latest-threat
set login-timestamp enable
set post-login-banner enable
set pre-login-banner enable
set radius-port 1812
set reset-sessionless-tcp disable
set special-file-23-support enable
end
```

6.7 SERVIDORES DE AUTENTICACIÓN

172. Las unidades FortiProxy soportan el uso de servidores externos de autenticación. Un servidor de autenticación puede proporcionar comprobación de contraseñas para un conjunto definido de usuarios de FortiProxy, o puede ser incluido como parte de un grupo de usuarios de FortiProxy.
173. **NOTA:** Si se va a proceder a la utilización de servidores de autenticación, estos han de ser configurados antes de configurar los usuarios o grupos de usuarios que harán uso de los mismos.

6.7.1 SERVIDORES SINGLE SIGN-ON

174. Fortinet hace uso de políticas de seguridad para controlar el acceso a recursos, basándose en grupos de usuarios configurados en las políticas correspondientes.
175. Cada grupo de usuarios de Fortinet es asociado con uno o más grupos de usuarios de *Service Directory*. Cuando un usuario se autentica en el dominio correspondiente (Windows o Novell), un agente FSSO (Fortinet *Single Sign-On*) envía la dirección IP del usuario, así como los nombres de los grupos de usuarios del *Service Directory* a los que dicho usuario pertenece, a la unidad FortiProxy.
176. El agente FSSO tiene dos componentes que han de ser instalados en el entorno de red:
- a) El agente de controlador de dominio (*domain controller agent*), que debe ser instalado en todos los controladores de dominio, con el fin de monitorizar procesos de *login* de usuarios, así como enviar información al respecto al agente recolector.

- b) El agente recolector (*collector agent*), que debe ser instalado en al menos un controlador de dominio, con el fin de enviar la información recibida por los agentes de controlador de dominio a la unidad FortiProxy.

177. La unidad FortiProxy usa esta información para mantener una copia de la base de datos de grupos de usuarios del controlador de dominio. Dado que el controlador de dominio autentica usuarios, la unidad FortiProxy no lleva a cabo autenticación. La unidad reconoce miembros de grupos por sus direcciones IP. Es necesario instalar el agente FSSO en la red, y configurar la unidad para obtener información del servidor de *Directory Service*.

178. Para llevar a cabo la gestión de servidores *Single Sign-On*, ir a **User & Device > Single Sign-On**.

+ Create New Edit Delete						
Name	Type	LDAP Server	Users/Groups	FSSO Agent IP/Name	Status	Ref.
No matching entries found						

Figura 12 – User & Device > Single Sign-On

179. Algunas de las opciones disponibles se enumeran a continuación:

- Crear: Crear un nuevo servidor FSSO.
- Editar: Editar un servidor FSSO.
- Eliminar: Eliminar uno o más servidores FSSO.

180. A continuación, se enumeran los pasos necesarios para crear un servidor SSO:

- En la lista de servidores de *Single Sign-On*, seleccionar **Create New** en la barra de herramientas.

Se abre la página **New Single Sign-On Server**.

New Single Sign-On Server

Type: Poll Active Directory Server
Fortinet Single-Sign-On Agent
RADIUS Single-Sign-On Agent

Server IP/Name:

User:

Password:

LDAP Server:

Enable Polling:

Figura 13- Nuevo servidor de Single Sign-On

- Seleccionar el tipo de servidor que se creará.

NOTA: Solo se puede crear un único agente de RADIUS SSO en la unidad FortiProxy.
- A continuación, introducir los datos correspondientes.

d) Seleccionar **OK** para crear el nuevo servidor.

181. A continuación, se enumeran los pasos necesarios para editar un servidor SSO:

- Seleccionar el servidor que se desea editar, y a continuación seleccionar **Edit** en la barra de herramientas. Se abrirá la ventana **Edit Single Sign-On Server**.
- Editar la información del servidor, y a continuación seleccionar **OK** para aplicar los cambios.

182. A continuación, se enumeran los pasos necesarios para eliminar un servidor SSO:

- Seleccionar el servidor o servidores que se desea eliminar.
- Seleccionar **Delete** en la barra de herramientas.
- Seleccionar **OK** en la ventana de confirmación para eliminar los servidores seleccionados.

6.7.2 SERVIDORES LDAP

183. Para llevar a cabo la gestión de servidores LDAP, ir a **Users & Device > LDAP Servers**.

+	Create New	Edit	Clone	Delete	Search	Q					
▼	Name	▼	Server	▼	Port	▼	Common Name Identifier	▼	Distinguished Name	▼	Ref.
	NewLDAPserver		7.8.9.0		389		cn		www.example.com		0

Figura 14 – Users & Device > LDAP Servers

184. A continuación, se enumeran los pasos necesarios para añadir un servidor LDAP.

- En la lista de servidores LDAP, seleccionar **Create New** en la barra de herramientas.

Se abrirá la ventana **Create LDAP Server**.

Create LDAP Server

Name

Server IP/Name

Server Port

Common Name Identifier

Distinguished Name

Bind Type Simple Anonymous Regular

Secure Connection

Figura 15 – Create LDAP Server

- A continuación, configurar los parámetros necesarios.
- Seleccionar **OK** para crear un nuevo servidor LDAP.

185. A continuación, se enumeran los pasos necesarios para editar un servidor LDAP:

- a) Seleccionar el servidor LDAP que se desea editar, y a continuación seleccionar **Edit** en la barra de herramientas.

La ventana **Edit LDAP Server** se abrirá.

- b) Editar la información del servidor como se desee, y a continuación seleccionar **OK** para aplicar los cambios.

186. A continuación, se enumeran los pasos para clonar un servidor LDAP:

- a) Seleccionar el servidor LDAP que se desea clonar.
- b) Seleccionar **Clone** en la barra de herramientas.
- c) Introducir un nombre para el servidor LDAP clonado en la ventana de diálogo, y seleccionar **OK**.
- d) Editar el servidor clonado como se desee.

187. A continuación, se enumeran los pasos para eliminar un servidor LDAP:

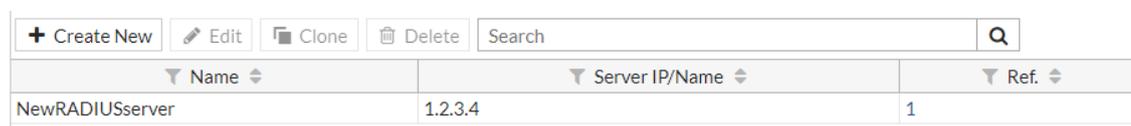
- a) Seleccionar el servidor o servidores que se desea eliminar.
- b) Seleccionar **Delete** en la barra de herramientas.
- c) Seleccionar **OK** en la ventana de confirmación para eliminar los servidores seleccionados.

6.7.3 SERVIDORES RADIUS

188. Se debe configurar el servidor RADIUS para aceptar la unidad FortiProxy como un cliente. Las unidades FortiProxy harán uso de las funcionalidades de autenticación y trazabilidad (*accounting*) del servidor RADIUS.

189. Cuando un usuario intenta acceder a la red, la unidad FortiProxy redirige la solicitud de autenticación al servidor RADIUS, quien lleva a cabo la comprobación de usuario y contraseña. Una vez que el proceso de comprobación se lleva a cabo con éxito, el servidor RADIUS envía el mensaje de “Autorización Concedida” a la unidad FortiProxy, que a continuación permitirá al usuario acceder a la red.

190. Para gestionar servidores RADIUS, ir a **User & Device > RADIUS Servers**.



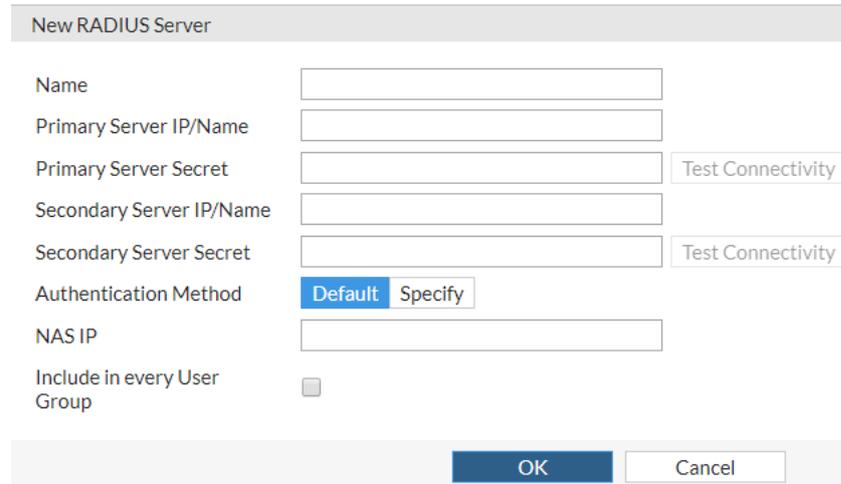
+ Create New Edit Clone Delete Search		
Name	Server IP/Name	Ref.
NewRADIUSserver	1.2.3.4	1

Figura 16 – User & Device > RADIUS Servers

191. A continuación, se enumeran los pasos para crear un servidor RADIUS:

- a) En la lista de servidores RADIUS, seleccionar **Create** en la barra de herramientas.

Se abrirá la ventana **New RADIUS Server**.



New RADIUS Server

Name

Primary Server IP/Name

Primary Server Secret Test Connectivity

Secondary Server IP/Name

Secondary Server Secret Test Connectivity

Authentication Method **Default** Specify

NAS IP

Include in every User Group

OK Cancel

Figura 17 – New RADIUS Server

- b) A continuación, configurar los parámetros necesarios.
- c) Seleccionar **OK** para crear un nuevo servidor RADIUS.

192. A continuación, se enumeran los pasos para editar un servidor RADIUS:

- a) Seleccionar el servidor RADIUS que se desea editar, y a continuación seleccionar **Edit** en la barra de tareas.

Se abrirá la ventana **Edit RADIUS Server**.

- b) Editar la información del servidor como se desee, y seleccionar **OK** para guardar los cambios.

193. A continuación, se enumeran los pasos para clonar un servidor RADIUS:

- a) Seleccionar el servidor RADIUS que se desea clonar.
- b) Seleccionar **Clone** en la barra de herramientas.
- c) Introducir un nombre para el servidor clonado, y seleccionar **OK** en la venta de diálogo correspondiente.
- d) Editar el servidor clonado como se desee.

194. A continuación, se enumeran los pasos para eliminar un servidor RADIUS:

- a) Seleccionar el servidor o servidores que se desea eliminar.
- b) Seleccionar **Delete** en la barra de herramientas.
- c) Seleccionar **OK** en la ventana de confirmación para eliminar el servidor seleccionado.

6.7.4 SERVIDORES TACACS+

195. Para gestionar servidores TACACS+, ir a **User & Device > TACACS+ Servers**.

Name	Server	Authentication Type	Ref.
NewTACACSserver	5.6.7.8	Auto	1

Figura 18 – User & Device > TACACS+ Servers

196. **NOTA:** Por defecto, la opción “TACACS+ Servers” no es visible, a no ser que se añada un servidor a través de la consola (CLI), empleando los siguientes comandos:

```
Config user tacacs+
  Edit <name>
    Set server <IP>
  Next
end
```

197. A continuación, se enumeran los pasos a seguir para añadir un servidor TACACS+:

- En la lista de servidores TACACS+, seleccionar **Create New** en la barra de herramientas.

Se abrirá la ventana **New TACACS+ Server**.

Figura 19 – New TACACS+ Server

- Seleccionar **OK** para crear el nuevo servidor TACACS+.

198. A continuación, se enumeran los pasos a seguir para editar un servidor TACACS+:

- Seleccionar el servidor TACACS+ que se desea editar, y a continuación seleccionar **Edit** en la barra de herramientas.

Se abrirá la ventana **Edit TACACS+ Server**.

- Editar la información del servidor como se desee, y seleccionar **OK** para aplicar los cambios.

199. A continuación, se enumeran los pasos para clonar un servidor TACACS+.

- Seleccionar el servidor TACACS+ que se desea clonar.
- Seleccionar **Clone** en la barra de herramientas.
- Introducir el nombre para el servidor TACACS+ clonado, y a continuación seleccionar **OK**.

d) Editar el servidor clonado como se desee.

200. A continuación, se enumeran los pasos a seguir para eliminar un servidor TACACS+.

- a) Seleccionar el servidor o servidores TACACS+ que se desea eliminar.
- b) Seleccionar **Delete** en la barra de herramientas.
- c) Seleccionar **OK** en la ventana de confirmación, para eliminar los servidores TACACS+ seleccionados.

6.7.5 KERBEROS

201. Kerberos es un método de autenticación empleado para autenticar usuarios de proxy web, tanto explícito como transparente.

202. Para configurar el servicio de autenticación Kerberos, ir a **User & Device > Kerberos**.

<input type="button" value="+ Create New"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>			
Name	Principal	LDAP Server	Ref.
NewKerberosAuth	www.testserver.com	NewLDAPServer	0

Figura 20 – User & Device > Kerberos

203. A continuación, se enumeran los pasos a seguir para añadir un nuevo servicio de autenticación Kerberos:

- a) En el listado de servicios de Kerberos, seleccionar **Create New** en la barra de herramientas.

Se abrirá la ventana **New Kerberos**.

New Kerberos

Name

Principal

LDAP Server

Keytab File

Figura 21 - New Kerberos

- b) A continuación, configurar los parámetros correspondientes.
 - **Name:** El nombre del servicio de autenticación a crear.
 - **Principal:** El nombre del Server Domain Name para el servicio de autenticación.
 - **LDAP Server:** El nombre del servidor LDAP empleado para el proceso de autorización.
- c) Seleccionar **OK** para crear el nuevo servicio.

204. A continuación, se enumeran los pasos a seguir para editar el servicio de autenticación Kerberos:

- a) Seleccionar el servicio que se desea editar, y a continuación seleccionar **Edit** en la barra de herramientas.

Se abrirá la ventana **Edit Kerberos**.

- b) Editar la información del servicio como se desee, y a continuación pulsar **OK** para aplicar los cambios.

205. A continuación, se enumeran los pasos a seguir para eliminar un servicio de autenticación Kerberos:

- a) Seleccionar el servicio o servicios que se desea eliminar.
- b) Seleccionar **Delete** en la barra de herramientas.
- c) Seleccionar **OK** en la ventana de confirmación, para eliminar los servicios seleccionados.

206. Para más información sobre servidores de autenticación, consultar el apartado "Authentication" de la Guía de Administración de FortiProxy [REF2].

6.8 SINCRONIZACIÓN AUTOMÁTICA DEL RELOJ

207. Es necesario mantener el reloj del equipo sincronizado con el del resto de equipos de la organización (como servidores de log, de autenticación, etc.). Esto posibilita trabajos de auditoría forense y consistencia en las fechas de caducidad usadas para verificar la expiración de certificados y protocolos de seguridad.

208. Para ello, se ejecutarán los siguientes comandos:

```
config system ntp
    set ntpsync enable
    set type custom
    config ntpserver
        edit 1
            set server
                <nombreDNS/direccionIP>
        next
    end
    set syncinterval 60
end
```

Donde **syncinterval** es el período de sincronización entre la unidad FortiProxy y el servidor NTP. El valor establecido puede situarse entre 1 y 1440 minutos.

209. Desde la interfaz web se puede configurar el reloj en **System > Settings > System Time**, aunque la totalidad de las opciones, entre las que se encuentra la configuración de servidores de tiempo personalizados, son únicamente accesibles mediante CLI.

6.9 BACKUP DE LA CONFIGURACIÓN

210. Una vez configurada la unidad FortiProxy y, sobre todo, antes de cualquier intervención que suponga un cambio en el equipo, es recomendable realizar un *backup* de la configuración, de modo que, ante un problema, sea posible retroceder a la configuración anterior.

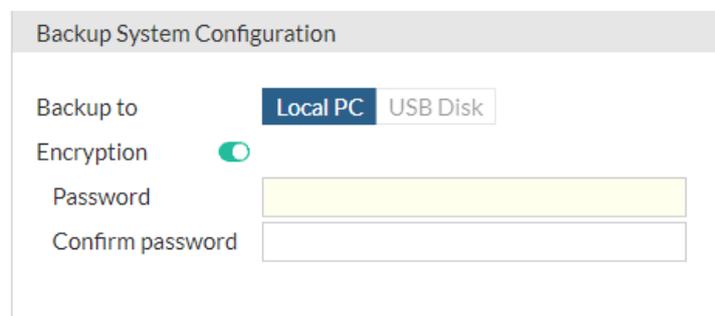
211. Cuando el sistema opera en modo de operación seguro, los *backups* de configuración no son compatibles con los realizados en otro modo de operación. Es decir, un *backup* del dispositivo en modo de operación seguro no puede ser restaurado cuando el dispositivo se encuentra en otro modo de operación y viceversa.

212. FortiProxy permite almacenar el *backup* en un PC local (equipo de administración), en un USB, o en un sitio FTP o TFTP (estos solo configurables vía CLI).

NOTA: Al ser los protocolos FTP y TFTP protocolos considerados inseguros, se desaconseja el uso de esta opción, recomendando las opciones de almacenamiento del backup en un equipo local o en un dispositivo USB.

213. Para la realización de *backups* de los ficheros de configuración mediante interfaz web se deberán seguir los siguientes pasos:

- a) Desplegar el menú que hay en la esquina superior derecha, y navegar hasta **Admin > Configuración > Backup**.
- b) Seleccionar donde se almacenará el *Backup* (PC local o USB).
- c) Seleccionar **Encryption**, esto pedirá introducir una contraseña, que será solicitada al restaurar el *backup*.
- d) Seleccionar **Backup**. Se solicitará la ruta donde almacenar el fichero de *backup* (con extensión .conf).



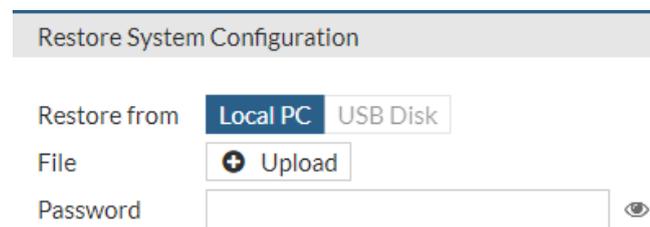
The screenshot displays the 'Backup System Configuration' window. At the top, the title is 'Backup System Configuration'. Below the title, there are four main sections: 'Backup to', 'Encryption', 'Password', and 'Confirm password'. The 'Backup to' section has two buttons: 'Local PC' (which is highlighted in blue) and 'USB Disk'. The 'Encryption' section has a green toggle switch that is turned on. The 'Password' and 'Confirm password' sections each have a text input field.

Figura 22 – Ejecución de Backups con FortiProxy

214. Se recomienda proteger los ficheros de *backup* de la configuración de acuerdo a la política de seguridad de la organización, y no emplear protocolos no seguros (sin cifrado) en la transmisión de éstos.

215. Para restaurar la configuración a través del interfaz web de gestión:

- a) Desplegar el menú que hay en la esquina superior derecha y navegar hasta **Admin > Configuration > Restore**.
- b) Seleccionar de dónde recuperará el *Backup* (PC local o USB). Introducir la ruta y nombre del fichero de configuración o seleccionarlo (**Upload**).
- c) Introducir la contraseña si se solicita.
- d) Seleccionar **Restore**.



Restore System Configuration

Restore from Local PC USB Disk

File

Password

Figura 23 – Restauración de Backup

6.10 AUTO-CHEQUEOS

216. Cuando el sistema está en modo de operación seguro, se realizan una serie de auto-chequeos (*self-tests*) durante el arranque del dispositivo. Estos incluyen: verificación de los mecanismos y funciones criptográficas a través de pruebas de respuesta conocida (*Known Answer Tests*, KAT), pruebas de integridad del firmware, y pruebas de *bypass* de configuración.

217. Por otra parte, el administrador también tiene la opción de realizar auto-chequeos de forma manual a través de los comandos introducidos en la consola CLI. Para realizar todos los test disponibles introducir por CLI el comando “**execute fips kat all**” o “**execute fips kat**” para realizar una comprobación específica.

218. Para realizar un test de forma individual ejecutar mediante CLI el comando “**execute fips kat <test_name>**”. En caso de querer visualizar una lista de los nombres de test disponibles, ejecutar el comando “**execute fips kat ?**”.

219. A continuación, se introduce un listado con los diferentes test que lleva a cabo el producto durante el arranque.

- a) Test de integridad del firmware empleando firmas RSA
- b) Test de integridad de la configuración, empleando HMAC SHA-256
- c) Test de respuesta conocida para cifrado, para el algoritmo AES, modo CBC
- d) Test de respuesta conocida para descifrado, para el algoritmo AES, modo CBC

- e) Test de respuesta conocida para HMAC SHA-1
- f) Test de respuesta conocida para SHA-1
- g) Test de respuesta conocida para HMAC SHA-256
- h) Test de respuesta conocida para SHA-256
- i) Test de respuesta conocida para HMAC SHA-512
- j) Test de respuesta conocida para SHA-512
- k) Test de respuesta conocida para generación de firma RSA
- l) Test de respuesta conocida para verificación de firma RSA
- m) Test de respuesta conocida para generación de firma ECDSA
- n) Test de respuesta conocida para verificación de firma ECDSA
- o) Test de respuesta conocida para DRGB
- p) Verificación del *boot loader*

220. Estos test aseguran la correcta operación de las funcionalidades criptográficas del producto, de la CPU y de la BIOS, así como la verificación de que se está usando una imagen íntegra del producto.

221. En caso de que alguno de los test falle, el dispositivo FortiProxy conmuta a un modo de error (*FIPS Error mode*). En este modo de error, se inhabilitan de forma automática todos los interfaces del dispositivo, incluyendo la consola, y se bloquea todo el tráfico. Para volver al modo de operación seguro, se debe apagar y encender de nuevo la unidad. En caso de que al iniciarse los test sean correctos, el dispositivo inicia el modo de operación seguro de forma normal. En caso de que los test continúen fallando significa que existe un problema grave en el firmware o en el hardware, y debe sacarse el dispositivo de la red hasta que el problema sea resuelto.

6.11 POLÍTICAS DE SEGURIDAD DEL PROXY

222. Los equipos FortiProxy se basan en tecnología *Stateful Inspection Packet*. Esto les permite hacer un análisis exhaustivo de la cabecera de cada paquete, identificando la sesión a la que pertenece, chequeando el correcto orden de los paquetes y realizando control sobre el tráfico de la red.

223. Las políticas de seguridad (***Security Policies***) o reglas del proxy, controlan todo el tráfico que atraviesa el equipo. Se definen en primer lugar en función del tipo de filtrado que se quiere realizar:

- a) **Explicit**: si se quieren realizar políticas de tipo proxy web explícito.
 - Permite habilitar el *proxy* explícito de tráfico IPv4 e IPv6 para HTTP y HTTPS en una o más interfaces. También admite el proxificado de sesiones FTP desde un navegador web y la configuración automática del proxy PAC (Proxy Auto-Config) para los usuarios del proxy web

explícito. Es necesario recordar que, entre otras acciones, un fichero PAC permite definir cómo un navegador web elegirá el servidor proxy que se empleará para recibir contenido HTTP. Además, también es posible admitir sesiones SOCKS desde un navegador web (sólo por CLI).

- Los *proxies* web explícito y FTP pueden funcionar al mismo tiempo en la misma o en distintas interfaces.
 - En su funcionamiento estándar, una vez recibida la sesión del navegador web, FortiProxy enruta la sesión a una interfaz de destino en función de su tabla de rutas, modificando la IP origen de la sesión utilizando para ello la dirección IP de la interfaz de salida (SNAT). Sin embargo, dicho comportamiento se puede modificar para mantener la IP original del cliente.
- b) **Transparent:** para realizar políticas de proxy firewall transparente.
- En este caso, aunque no soporta tantas funcionalidades como el modo explícito, no es necesario modificar nada en el sistema del usuario, ni reconfigurar su navegador o publicar un fichero PAC.
 - Este modo sí permite la autenticación al tráfico HTTP aceptado por una política.
 - En aquellas redes donde no se pueda realizar autenticación basada en IP, sí se podría utilizar el proxy transparente para aplicar autenticación basada en el navegador del usuario, pudiendo discernir los distintos usuarios incluso si se conectan a través de la misma IP.
- c) **FTP:** para políticas de proxy FTP explícito.
- Es posible habilitar el proxy FTP explícito en una o varias interfaces. De hecho, los *proxies* web explícitos y FTP pueden funcionar al mismo tiempo en la misma o en distintas interfaces.
 - Una vez que el proxy FTP recibe la sesión de FTP, FortiProxy enruta la sesión a una interfaz de destino en función de su tabla de rutas, modificando la IP origen de la sesión utilizando para ello la IP de la interfaz de salida (SNAT).
- d) **SSH Tunnel:** Para políticas de seguridad y control sobre el tráfico en el que un servidor SSH hace de proxy de este protocolo, redireccionándolo a otro servicio como puede ser RDP (*Remote Desktop Protocol*), VNC (*Virtual Network Computing*) o incluso HTTP/s. El servidor SSH encapsula y cifra el tráfico para garantizar su confidencialidad e integridad.
- e) **SSH Proxy:** Políticas de seguridad y control de tráfico para sesiones SSH utilizando FortiProxy como reenviador.
- f) **Wanopt:** para túneles de optimización WAN.
- El tráfico optimizado puede pasar entre varios equipos FortiProxy o

entre un FortiClient y un FortiProxy a través de un túnel de optimización WAN. El tráfico en el túnel puede ser enviado en texto plano o encriptado usando AES-128bit-CBC SSL, por lo que **se recomienda utilizar esta segunda opción para maximizar la seguridad**. Tanto el texto plano como los túneles cifrados utilizan el puerto de destino TCP 7810. Es necesario indicar que, por defecto, el tráfico que circula por el túnel se envía cifrado.

NOTA: Si bien se ha indicado que por defecto el tráfico que circula por el túnel se envía cifrado, los administradores tienen la opción de configurar si este circula en texto plano o cifrado.

- Antes de iniciar un túnel, se deben configurar los *peers* (pares) para autenticarse entre sí. A continuación, el *peer* del lado del cliente intentará iniciar un túnel de optimización WAN con el peer del lado del servidor. Una vez que los pares se autenticuen entre sí, se pondrá en marcha el túnel y se iniciará la comunicación de optimización de la WAN a través del él. Una vez establecido el túnel, pueden iniciarse y detenerse múltiples sesiones de optimización WAN entre *peers* sin reiniciar el túnel.

224. Estos tipos de políticas vienen detallados en **FortiProxy Administration Guide [REF2], sección Policy & Objects**.

225. Las políticas de seguridad (**Security Policies**) o reglas del *proxy* se definen también en base a los interfaces de entrada y salida, al origen (dirección IP o usuario) y a la dirección IP o servicio de internet de destino. Permiten seleccionar, también, un rango temporal (*Schedule*) y una aplicación/servicio/protocolo. Esta organización permite que el paquete sea procesado, comenzando por la política superior de todas y descendiendo hasta encontrar aquella con la que coincida en función de los diferentes parámetros de la política. **Deberá dejarse la política por defecto a Bloqueo (Deny), e ir añadiendo las políticas específicas por encima**, recomendando situar las más específicas arriba y las más generales abajo.

226. A la hora de configurar las reglas y políticas del *proxy*, siempre debe seguirse el principio de mínima funcionalidad y mínimo privilegio, de modo que sólo se permita el tráfico necesario y no otro, en la franja horaria necesaria.

227. Las políticas se definen desde el interfaz web en **Policy&Objects > Policy**

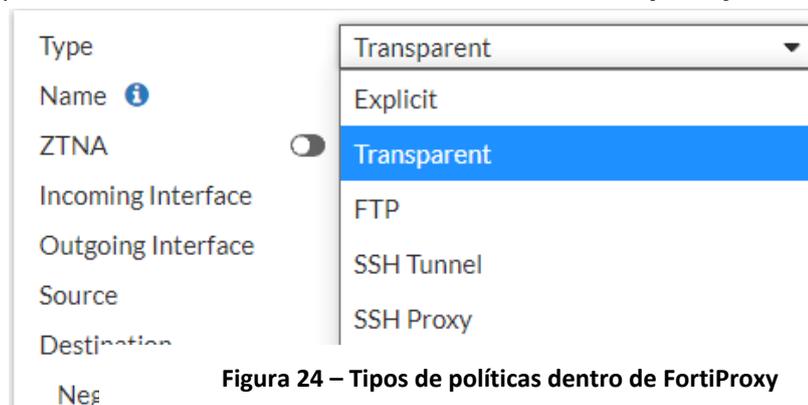


Figura 24 – Tipos de políticas dentro de FortiProxy

228. Es posible definir los interfaces de entrada y salida de tráfico como **Any**, para así poder inspeccionar un flujo de tráfico concreto independientemente de cuales sean sus interfaces de entrada o salida.
229. **Únicamente se utilizará la variable *any* cuando esté debidamente justificado y la complejidad asociada a establecer un conjunto de reglas individuales sea un riesgo mayor que el uso de este objeto. Si no es necesario y se puede especificar el origen o destino, no deberá utilizarse.** Un ejemplo en que esta complejidad podría afectar a la seguridad puede darse cuando, tratando de obviar el uso de esta variable, se hace necesario crear un número enorme de políticas. De esta forma, la gestión del Proxy puede incurrir en más problemas de seguridad que con una sola regla con el valor ***any*** en origen/destino.

6.12 PERFILES DE SEGURIDAD

230. Mientras que las políticas de seguridad del *proxy* proporcionan las instrucciones al dispositivo para controlar el tráfico al que se permite pasar a través de él, los perfiles de seguridad (***Security Profiles***) establecen los filtros que se deben aplicar al contenido del tráfico permitido por las políticas.
231. Un perfil de seguridad es un conjunto de instrucciones y filtros que pueden aplicarse sobre una o varias políticas de seguridad. Existen perfiles de seguridad para la detección de varios tipos de tráfico no deseado y amenazas a la red. Cada uno de ellos se configura de forma separada y se aplica a la política cuando esta se crea.
232. Los siguientes perfiles de seguridad están disponibles en Fortipoxy:
- a) **Antivirus (AV)**. Es el perfil de seguridad que se utiliza para la protección contra la transmisión de código malicioso, referido normalmente como *malware* (troyanos, virus, gusanos, *exploits* de puerta trasera, *spyware*, *radware*, etc.)
 - Escaneo de virus.
 - Protección contra *grayware*.
 - Escaneo heurístico.
 - Protección contra *phishing*.
 - Protección contra *botnets*.
 - Inspección de ficheros sospechosos.
 - b) **Filtrado Web (Web Filtering)**. Es el perfil de seguridad que se utiliza para proteger de URLs y contenidos web no apropiados.

El orden en que la unidad FortiProxy aplica los filtros web al tráfico, es el siguiente:

- Filtrado URL.
- Filtrado en función de las categorías FortiGuard.

- Filtrado de contenidos y scripts web.
- Escaneo antivirus.
- c) **Control de Aplicaciones (*Application Control*)**. Es el perfil que se utiliza para determinar qué aplicaciones pueden operar en la red, y para restringir el uso de estas aplicaciones según se requiera.
- d) **IPS (*Intrusion Protection*)**. Es el perfil que se utiliza para proteger la red de actividades o comportamientos que concuerdan con técnicas de ataque.
- e) **DLP (*Data Leak Prevention*)**. Es el perfil que se utiliza para prevenir que información sensible pueda salir fuera de la red interna.
- f) **Filtrado DNS (*DNS Filter*)**. Es el perfil que se utiliza para bloquear las peticiones DNS realizadas sobre direcciones de *Botnet* o servidores C&C conocidos por FortiGuard.
- g) **Análisis de Contenido (*Content Analysis*)**. Es el perfil que se utiliza para la detección de contenido para adultos en imágenes.
- h) **SSL/SSH Inspection**. Es el perfil que se utiliza para poder escanear el tráfico HTTPS de la misma manera que se puede hacer en HTTP.
- i) **Proxy Options**. Es el perfil que incluye características que puede configurar para cuando su FortiProxy esté funcionando en modo proxy, incluyendo la asignación de puertos de protocolo, el bloqueo de archivos/correos electrónicos de gran tamaño y otras opciones de web y correo electrónico.

6.12.1 ANTIVIRUS

233. El Perfil de Seguridad Antivirus (**AV Profile**) utiliza una suite de tecnologías de seguridad integradas, que proporcionan protección contra una variedad de amenazas, incluyendo códigos conocidos o desconocidos (*malware*) y APTs (*Advanced Persistent Threats*).
234. En el perfil de AV se puede configurar que la unidad FortiProxy aplique la protección antivirus a las sesiones HTTP, SMTP, POP3, IMAP, MAPI, FTP y CIFS. En caso de que, además, el modelo soporte la inspección de contenido SSL, se puede configurar la protección antivirus para las sesiones HTTPS, IMAPS, POP3S, SMTPS, y FTPS. El motor de escaneo AV utiliza una base de datos de firmas de virus (*signature database*) en la que se detallan los atributos únicos de cada infección. El escáner AV busca estas firmas y cuando las encuentra, la unidad FortiProxy determina que el fichero ha sido infectado y toma la acción configurada en el perfil AV.
235. Todas las unidades FortiProxy disponen de la base de datos de firmas denominada *Normal*. Los modelos físicos y los virtuales con más de 8GB de RAM disponen de otras dos bases de datos adicionales: *Extended* y *Extreme*:
- a) **Normal**: contiene las firmas de los virus más habituales en la actualidad.
 - b) **Extended**: suma a la base de datos normal, los virus del último año.

- c) **Extreme**: añade a la base de datos *extended*, una amplia colección de virus antiguos y con escasa o nula actividad durante los últimos años.

236. La selección de la base de datos depende de las necesidades de la organización. La cobertura más completa corresponde a *Extended*, pero requiere un coste adicional en recursos de procesamiento.

237. La selección de la base de datos solo se puede realizar a través de CLI:

```
config antivirus settings
    set default-db extended
end
```

238. Las técnicas que puede utilizar el AV son: escaneo de virus, protección *grayware*, escaneo heurístico, y, en el caso de disponer del servicio FortiGuard, este permite la protección *botnet*, detectando y bloqueando intentos de conexión a *botnets* conocidas, y a sitios de *phishing* conocidos. La base de datos de FortiGuard es actualizada continuamente con direcciones de sitios de mando y control (*C&C sites*) a los que los clientes *botnet* intentan conectarse, y con direcciones conocidas de URLs de *phishing*.

239. Otra funcionalidad que se puede incorporar en el perfil de seguridad AV es la inspección de ficheros sospechosos, en FortiSandbox. Cuando FortiProxy detecte algún fichero sospechoso, lo enviará a un *appliance* FortiSandbox (si se dispone de él) o a FortiSandbox en la nube (si se dispone del servicio en FortiCloud). Si FortiSandbox, tras testear el fichero determina que exhibe un comportamiento malicioso o contiene virus, se crea una nueva firma en la base de datos de firmas de FortiProxy.

240. Las actualizaciones automáticas del motor antivirus y de la base de datos de firmas, se realizan diariamente y se distribuyen mediante *FortiProtect Distribution Network* (FDN). Esta red está compuesta por servidores distribuidos en todo el mundo, y que son seleccionados por el dispositivo en función de la zona horaria configurada.

241. Se soportan tres modos de actualización:

- a) **Pull updates**. Los equipos comprueban automáticamente si existen en la red FDN nuevas definiciones de virus disponibles y, si encuentran nuevas versiones, las descargan y las instalan automáticamente, así como los motores de antivirus actualizados. Estas comprobaciones pueden ser programadas para su realización en periodos horarios, diarios o semanales.
- b) **Push updates**. Cada vez que un nuevo motor de antivirus o nuevas definiciones son publicadas, los servidores que forman parte de la red FDN notifican a todos los equipos FortiProxy configurados para *push updates*, que una nueva actualización está disponible. En 60 segundos desde la recepción de una notificación *push*, el equipo se descargará la actualización desde la FDN.

- c) **Manual.** El administrador del equipo inicia la actualización con la opción **System>FortiGuard>update now** desde la consola de gestión o mediante el siguiente comando desde CLI:

```
Exe update-now
```

242. La configuración del perfil de seguridad AV se realiza desde **Security Profiles > AntiVirus**. Se recomienda disponer de un perfil de seguridad AV por defecto y aplicarlo de forma general a las políticas, que bloquee todos los virus detectados para todos los protocolos y, en caso de disponer del servicio, envíe todos los ficheros a FortiSandbox para inspección.
243. Para más información sobre la configuración de estos perfiles de seguridad, consultar el capítulo “*Security Profiles*” de *Fortipoxy Administration Guide* [REF2].

6.12.2 FILTRADO WEB

244. El perfil de seguridad de Filtrado Web (**Web Filter**) realiza el filtrado del tráfico HTTP. Para ello, comprueba la dirección de destino de las peticiones HTTP/S. Las tres funciones principales de este filtrado son: filtrado de URLs, filtrado de contenido web y, en caso de disponer del servicio, filtrado por categorías de FortiGuard.
245. El orden en que la unidad FortiProxy aplica los filtros web al tráfico, es el siguiente:
- Filtrado URL.
 - Filtrado en función de las categorías FortiGuard.
 - Filtrado de Contenidos y Scripts web.
 - Escaneo antivirus.
246. En primer lugar, el filtrado URL permite bloquear o permitir URLs específicas añadiéndolas a una lista de filtrado estático de URLs (*Static URL Filter List*). Para añadir las URLs se pueden utilizar patrones que contienen texto, comodines o expresiones regulares. **Siempre que sea posible, se deberán utilizar las listas blancas en lugar de listas negras.**
247. Las acciones que se pueden realizar son: *Allow*, *Block*, *Monitor* y *Exempt*. Bloquear impide el tráfico desde la URL y muestra en su lugar un mensaje al usuario. Permitir y Monitorizar, dan acceso a la URL y continúan con la aplicación de todos los demás perfiles de seguridad sobre el tráfico (incluido antivirus). En caso de Monitorizar se genera, además, un mensaje de log. El caso de Eximir (*Exempt*) no solo permite el acceso a la URL, sino que no aplica ningún otro escaneo al tráfico. **No se recomienda utilizar la acción “Eximir”. En su lugar, deberá utilizarse la acción “Monitorizar”.**
248. La función de filtrado de contenido web, permite bloquear el acceso a páginas web que contengan patrones determinados. Estos se pueden especificar mediante palabras (*Banned Words*), frases, patrones, comodines y expresiones regulares en lenguaje Perl. El filtrado de contenido incluye la detección de scripts y códigos

maliciosos, para permitir el bloqueo de contenido web inseguro, tal como Java Applets, Cookies y ActiveX.

249. En caso de disponer del servicio de filtrado Web de FortiGuard, se pueden escoger las categorías a filtrar de entre todas las ofrecidas por FortiGuard, que recopila billones de páginas web categorizadas.

250. La configuración de los perfiles de Filtrado Web se realiza desde **Security Profiles**

> **Web Filter**. Se recomienda disponer de un perfil de filtrado Web por defecto, asociado a la política de seguridad que gobierna el acceso a Internet (la cual debe tener habilitada, también, la inspección SSL), con modo de inspección *Proxy- Based*, y con listas de filtrado URL y filtrado de contenidos.

251. Para más información sobre la configuración de estos perfiles de seguridad, consultar el capítulo “*Security Profiles*” de *FortiProxy Administration Guide* [REF2].

The screenshot displays the configuration for a new Web Filter Profile. At the top, there's a 'New Web Filter Profile' header. Below it, there are input fields for 'Name' and 'Comments' (with a character count of 0/255), and a 'Log all URLs' toggle. The main section is 'FortiGuard Category Based Filter', which is currently turned on. It features a table with columns 'Name' and 'Action'. The table is divided into two sections: 'Local Categories' (2 items) and 'Potentially Liable' (10 items). The 'Local Categories' section shows 'custom1' and 'custom2', both with a 'Disable' action. The 'Potentially Liable' section shows categories like 'Drug Abuse', 'Hacking', 'Illegal or Unethical', and 'Discrimination', all with an 'Allow' action. Below the table, there are several toggle options: 'Allow users to override blocked categories' (off), 'Static URL Filter' (off), 'Block invalid URLs' (off), 'URL Filter' (off), 'Block malicious URLs discovered by FortiSandbox' (off), 'Content Filter' (off), 'Rating Options' (off), 'Allow websites when a rating error occurs' (off), 'Rate URLs by domain and IP Address' (off), 'Proxy Options' (off), 'HTTP POST Action' (set to 'Allow'), and 'Remove Cookies' (off).

Figura 25 – Perfil de filtrado Web

6.12.3 CONTROL DE APLICACIONES

252. El perfil de seguridad de Control de Aplicaciones (***Application Control***), permite que FortiProxy detecte y tome las acciones correspondientes sobre un tráfico de red, en función de la aplicación que lo ha generado. Hace uso de los decodificadores de protocolo de la función IPS de FortiProxy, que pueden analizar el tráfico para detectar su correspondencia a determinadas aplicaciones, incluso aunque no utilicen puertos y protocolos estándar.

253. Para cambiar los puertos a examinar por un decodificador IPS, ha de usarse la consola (CLI). A continuación, se muestra el comando a emplear para examinar los puertos asociados a una aplicación.

```
Config ips decoder <nombre_decodificador>
    Set port_list "<listado de puertos>"
end
```

254. Es necesario indicar que no se podrán modificar los puertos de decodificadores IPS que por defecto tengan asignado dicho valor a "**auto**". Estos decodificadores pueden detectar el tipo de tráfico configurado en cualquier puerto, por lo que no es necesario especificar puertos concretos.

255. La unidad FortiProxy incluye una lista de firmas que identifican más de 2500 aplicaciones, servicios y protocolos. A través del servicio de control de aplicaciones de FortiGuard, se pueden actualizar nuevas firmas para detectar nuevas aplicaciones.

256. La base de datos de firmas de aplicaciones que tiene la unidad FortiProxy, se puede ver desde **Security Profiles > Application Control** en el botón de la esquina superior derecha (*View Application Signatures*). Esto abre una ventana que muestra una lista de firmas compuestas por las siguientes columnas: nombre, categorías (*Business, Botnet, Collaboration, Audio/Video, etc.*), Tecnología (*Browser Based, Client-Server, Peer-to-Peer*), Popularidad (de 1 a 5 estrellas), Riesgo (tipo de impacto que provocaría permitir el tráfico de esa aplicación: *Malware or Botnet, Bandwidth Consuming o None*).

Figura 26 – Perfil de Application Control

257. Las acciones a realizar cuando se detecta el tráfico de una aplicación filtrada son: *Block*, *Allow*, *Monitor* y *Quarantine* (bloquea la aplicación durante un tiempo configurable, siendo el período máximo de un año).
258. El perfil de seguridad de Control de Aplicaciones se configura desde **Security Profiles > Application Control**. Se recomienda identificar las aplicaciones que se utilizan en la organización y que, por lo tanto, estén permitidas por la política de seguridad, y crear un perfil por defecto, que bloquee todas las aplicaciones, excepto esas.
259. Para más información sobre la configuración de estos perfiles de seguridad, consultar el capítulo “*Security Profiles*” de *FortiProxy Administration Guide*[REF2].

6.12.4 PROTECCIÓN FRENTE A INTRUSIONES (IPS)

260. A través de los perfiles de seguridad de IPS (*Intrusión Protection*), FortiProxy proporciona detección y prevención de ataques utilizando dos técnicas: detección basada en firmas y detección basada en anomalías. La base de datos de firmas que tiene la unidad FortiProxy o cualquier firma adicional que hayamos creado, se puede ver en **Security Profiles > Intrusion Protection > View IPS Signatures**.

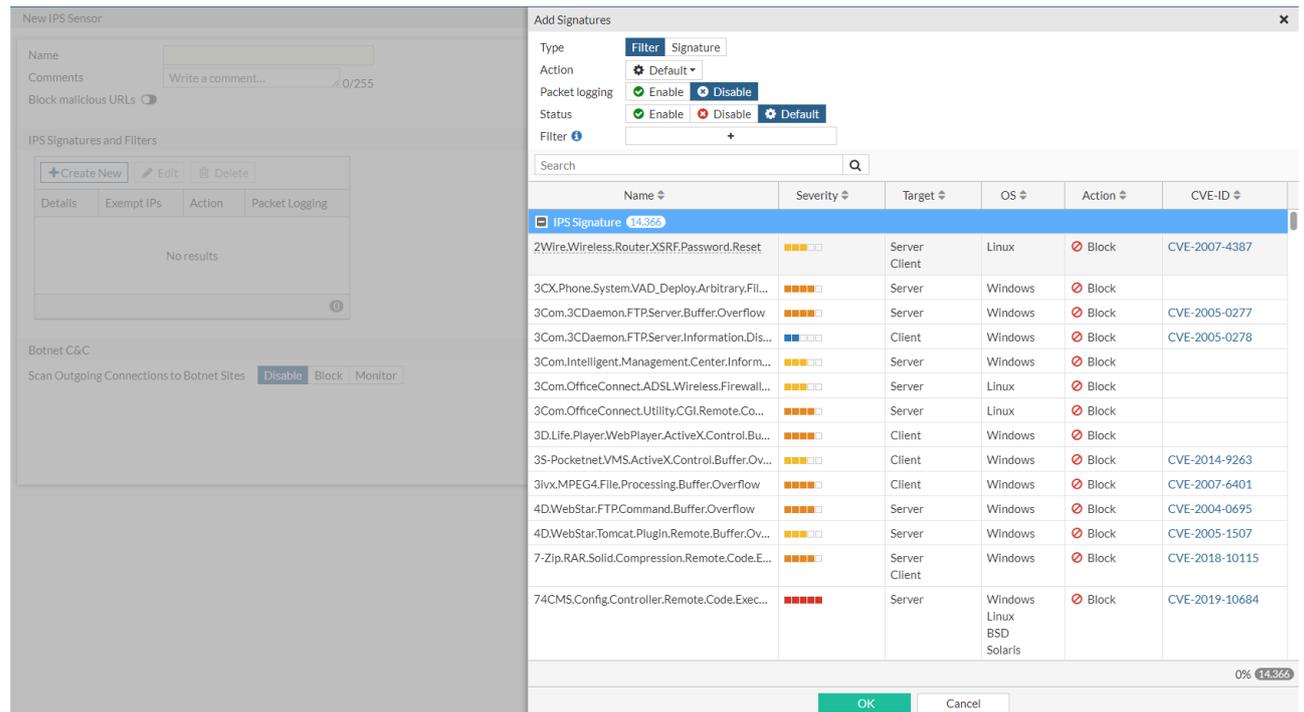


Figura 27 – Configuración del Sensor IPS

261. El motor IPS proporciona decodificadores de protocolo para el tráfico a analizar. Esto permite que, en el caso de ataques que solo afectan a un protocolo, FortiProxy buscará la firma del ataque únicamente en el tráfico que corresponda a ese protocolo.
262. La definición de las firmas que se van a buscar en determinado tráfico, se realiza a través de los Sensores IPS, los cuales detectan comportamientos anómalos o maliciosos en una comunicación. A su vez, cada sensor dispondrá de uno a varios Filtros IPS, que corresponden a una colección de firmas. Estas firmas se pueden especificar de la siguiente forma:
- Basadas en Patrones (*Pattern Based*)**, seleccionando los atributos asociados con el tipo de ataque: aplicación afectada por el ataque, sistema operativo, protocolo (usado como vector de ataque), Severidad (nivel de amenaza) y objetivo (target).
 - Basadas en puntuación (*Rate Based*)**. En la base de datos de firmas, suelen existir unas firmas por defecto con la acción asociada de “Monitor” en lugar de bloquear. Estas son firmas de ataques que solo se consideran una amenaza importante si son recurrentes. En cualquier caso, es posible analizar los logs para tomar una determinación sobre ellas.
 - Customizadas**. Especificación manual.
263. Los sensores IPS pueden ser seleccionados en **Security Profiles > Intrusion Prevention**. Una vez creados, pueden ser añadidos a las diferentes políticas de seguridad. Cada uno de ellos contiene una configuración completa basada en firmas conocidas.

264. A continuación, se enumeran los pasos indicados para crear un sensor IPS.
- Desde la lista de sensores IPS, seleccionar **Create New**.
 - Introducir el nombre del nuevo sensor IPS.
 - Opcionalmente, introducir un comentario. Dicho comentario aparecerá reflejado en la lista de sensores IPS.
 - Añadir firmas conocidas individuales, o usar un filtro IPS para añadir múltiples firmas al sensor, especificando para ello las características de las firmas que se desea añadir.
 - Activar el botón **Enable** en la tabla **Rate Based Signatures**, para cada firma que se desea habilitar.
 - Seleccionar **OK** para crear el sensor IPS.
265. Las acciones que se pueden configurar cuando se detecta una concordancia con una firma, son: *Pass* (permite el tráfico), *Monitor* (permite el tráfico y registra la actividad), *Block* (descarta el tráfico), *Reset* (cierra la sesión), *Quarantine* (rechaza el tráfico de esa IP origen durante un tiempo configurable).
266. Se puede habilitar en los filtros la opción de *Packet Logging*, para que FortiProxy guarde una copia de todos los paquetes que coinciden con cualquiera de las firmas IPS del filtro, y poder analizarlos posteriormente. Sin embargo, esto debe hacerse con cautela, ya que aquellos filtros configurados con pocas restricciones pueden contener miles de coincidencias de firmas, y generar una inundación de paquetes en el log. Esta herramienta de *Packet Logging* está pensada para usar en situaciones determinadas y con un alcance acotado.
267. La actualización del motor y de las firmas IPS predefinidas se hace a través del servicio FortiGuard, al igual que Antivirus. Se puede configurar la actualización automática cada cierto tiempo en **System > FortiGuard > AntiVirus & IPS Updates > Enable Scheduled Updates**.

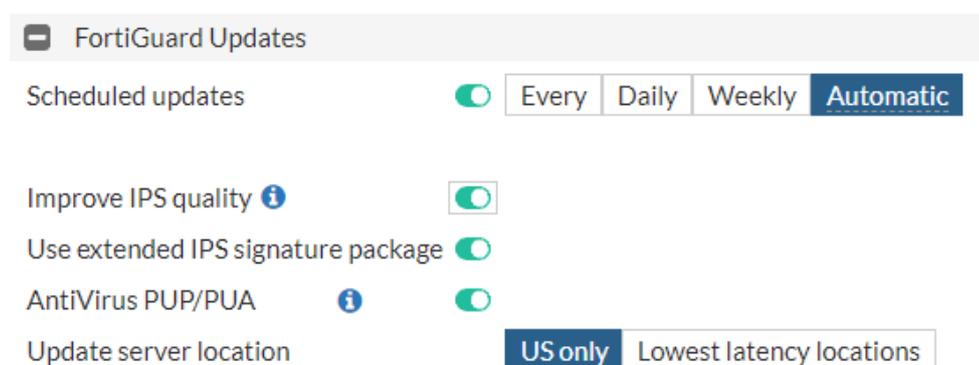


Figura 28 – Actualización programada de firmas

268. El perfil de seguridad de IPS se configura desde **Security Profiles > Intrusion Protection** (Ver Figura 25). Se recomienda crear un perfil por defecto, que bloquee todo el tráfico que coincida con las firmas de los filtros configuradas, e ir permitiendo progresivamente aquellas firmas que generen falsos positivos.
269. Para más información sobre la configuración de estos perfiles de seguridad, consultar el capítulo “*Security Profiles*” de *FortiProxy Administration Guide*[REF2].

6.12.5 DLP

270. La característica del Perfil de Seguridad Prevención de Fuga de Información o **DLP (Data Leak Prevention)** permite filtrar los datos que pasan a través de la unidad FortiProxy, para evitar que la información considerada sensible o confidencial, salga fuera de la organización. Esto se hace a través de la definición de patrones de datos sensibles, de forma que aquellos que pasen a través de FortiProxy, serán detectados y bloqueados, o permitidos y registrados (*logged*).
271. Para realizar el filtrado, se definen Sensores DLP que se aplican a las políticas de seguridad. Cada sensor DLP está compuesto de uno o varios filtros DLP, que son los que definen los patrones que se deben buscar en el tráfico. Cuando se encuentra una concordancia con los filtros definidos, las acciones a realizar son: *Allow*, *Log Only* (permite y genera un mensaje de log), *Block* y *Quarantine* (bloquea el tráfico de la IP origen durante un tiempo configurable).
272. La unidad FortiProxy dispone de un conjunto de sensores DLP preconfigurados que pueden editarse para adaptarlos a nuestras necesidades. Un sensor por defecto es, por ejemplo, “*Credit-Card*” que registra (*log*), tanto ficheros como mensajes, que contienen números de tarjetas de crédito en los formatos usados por American Express, MasterCard y Visa.
273. Para especificar los filtros DLP se pueden usar variables como tamaño de ficheros, tipos de fichero, expresiones regulares, si el fichero está cifrado o no, patrones, etc. Permite también realizar *fingerprinting*, calculando un *checksum* del fichero que deseamos detectar (solo para unidades FortiProxy que disponen de espacio de almacenamiento).
274. El filtrado DLP se puede utilizar también para dejar registro de actividades, de forma que al habilitar el archivado en un sensor DLP, la unidad FortiProxy va a dejar registro en el log, de todos los mensajes que coincidan con los filtros del sensor. Se puede archivar en modo resumen (*Summary*) de forma que solo se deja un resumen del mensaje, o en modo Total (*Full*) de forma que registra el mensaje al completo. Por ejemplo, para el primero, en el caso de un email sólo almacenaremos sus cabeceras, por su parte, en modo Full almacenaremos el propio mensaje incluidos sus adjuntos, lo que resulta en un incremento del almacenamiento y procesamiento.
275. El perfil de seguridad de DLP se configura desde **Security Profiles > Data Leak Prevention**. Se recomienda crear un perfil por defecto, que bloquee cualquier tráfico relacionado con información que tengamos clasificada como no pública.

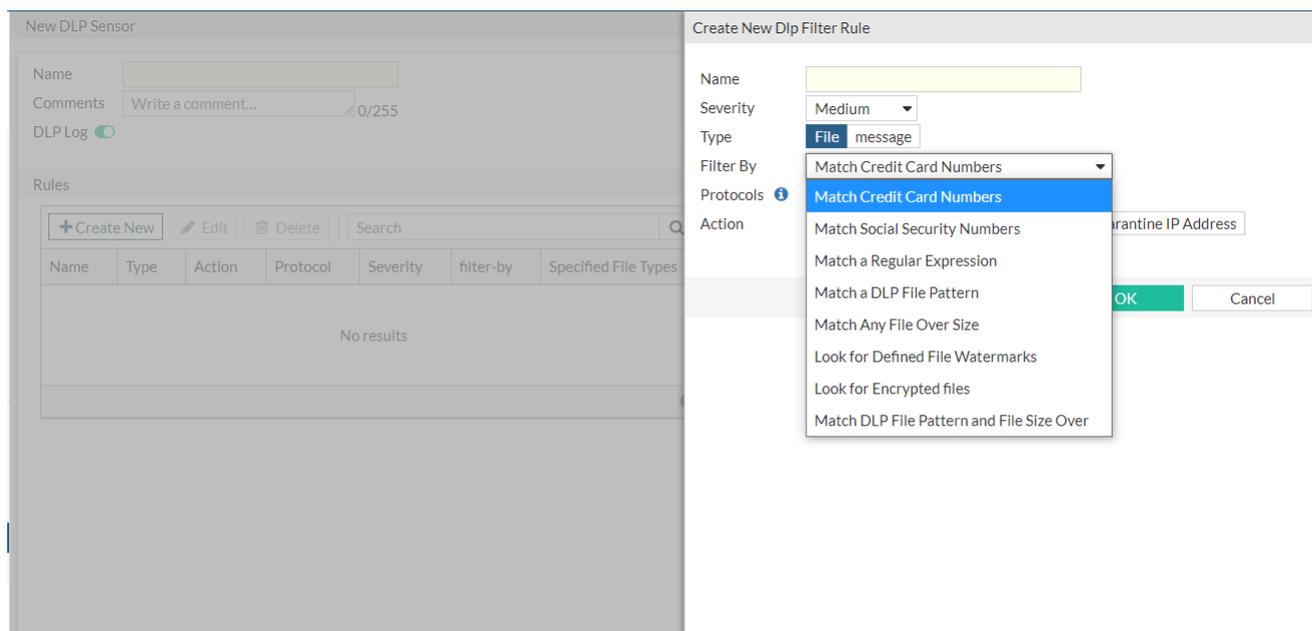


Figura 29 – Configuración de perfiles DLP

276. Para más información sobre la configuración de estos perfiles de seguridad, consultar el capítulo “*Security Profiles*” de *FortiProxy Administration Guide* [REF2].

6.12.6 CONTENT ANALYSIS

277. A través de los perfiles de seguridad de análisis de contenido (**Content Analysis**), FortiProxy proporciona una IA de visión automatizada que detecta amenazas visuales, como la pornografía, el extremismo y la violencia gráfica. El análisis de contenidos dota a la aplicación de una moderación de contenidos mediante IA que reconoce las amenazas en las imágenes.

278. Una vez detectado contenido inapropiado, dicho contenido puede ser opcionalmente bloqueado o reportado.

279. Las imágenes que se pueden categorizar en un perfil de Análisis de Contenido son: alcohol, drogas, extremismo, apuestas, contenido violento, pornografía, ropa interior y armas. Si una imagen de estas características es detectada, esta puede ser bloqueada, monitorizada, o sustituida por otra.

280. El perfil de seguridad de **Content Analysis** se configura desde **Security Profiles > Content Analysis** (ver Figura 4). Se recomienda crear un perfil por defecto, que bloquee cualquier tráfico relacionado con imágenes de las categorías que puede tratar.

281. Para más información sobre la configuración de estos perfiles de seguridad, consultar el capítulo “*Security Profiles*” de *FortiProxy Administration Guide*[REF2].

6.12.7 INSPECCIÓN DEL TRÁFICO SSH/SSL

282. FortiProxy permite la creación de perfiles para la inspección del tráfico SSH/SSL. Esta inspección permite aplicar escaneo antivirus, filtrado web, y filtrado de aplicaciones al tráfico cifrado. Para ello, la unidad FortiProxy:

- a) Intercepta y descifra las sesiones HTTPS, IMAPS, POP3S, SMTPS, y FTPS entre clientes y servidores.
- b) Aplica la inspección de contenido a los datos descifrados, empleando para ello las funcionalidades de Antivirus, DLP, archivado DLP, Filtrado Web (a las sesiones HTTPS) y filtrado Anti-Spam (a las sesiones IMAPS, POP3S, y SMTPS).
- c) Cifra la sesión de nuevo, y la reenvía a su destino.

283. Se puede especificar que ciertos sitios web no sean inspeccionados añadiéndolos a la lista de *“Exempt from SSL Inspection”*, dentro del perfil de inspección correspondiente. Por defecto, la unidad FortiProxy marca como exentas las categorías de: *Health and Wellness, Personal Privacy, Finance and Banking*. Si se dispone del servicio FortiGuard, éste proporciona una lista de dominios con buena reputación que pueden ser excluidos de la inspección SSL, y que periódicamente actualiza en las unidades FortiProxy.

284. Hay dos modos de inspección SSL:

- a) **Full o Deep Inspection**, que inspecciona todo el tráfico SSL.
- b) **SSL Certificate Inspection**, que solo inspecciona el certificado y verifica que esté correctamente firmado y vigente, no los contenidos del tráfico.

285. A su vez, el modo de *Full Inspection* permite, también, dos modos de inspección:

- a) Múltiples clientes que se conectan a múltiples servidores: para políticas genéricas en las que el destino es desconocido.
- b) Protección de Servidores SSL: perfiles personalizados para servidores SSL concretos con un certificado específico que hacen uso de Extended Key Usage para su autenticación (con la opción *“Web Server Authentication”* habilitada).

286. A la hora de crear un perfil de inspección SSL, debe seleccionarse el certificado que va a utilizar la unidad FortiProxy. Se recomienda utilizar un certificado emitido por una CA de confianza en el que los clientes confiarán (ya tendrán el *CA root certificate* en su almacén de certificados). También puede utilizarse un certificado auto-firmado (*self-signed*), en cuyo caso será necesario desplegarlo en todos los clientes para no generar errores de certificado. No obstante, esta última opción se desaconseja.

287. El perfil de inspección SSL/SSH se configura desde **Security Profiles > SSL/SSH Inspection**. Se recomienda crear un perfil por defecto con modo de inspección **Full**

Inspection, que permita inspeccionar todo el tráfico SSL y aplicar los filtros antivirus, DLP, filtrado Web.

Figura 30 – Configuración de Perfil SSL/SSH

288. Para más información sobre la configuración de estos perfiles de seguridad, consultar el capítulo “Security Profiles” de FortiProxy Administration Guide [REF2].

6.12.8 FILTRADO DNS

289. El Perfil de Seguridad de filtrado DNS (**DNS Filter**) se utiliza para permitir, bloquear o monitorizar el acceso a contenido web de acuerdo con las categorías FortiGuard. Cuando el filtrado DNS está habilitado, la unidad FortiProxy utiliza el servicio de resolución DNS de FortiGuard. Las peticiones de resolución DNS (*DNS lookups*) enviadas al servicio DNS de FortiGuard, devuelven una dirección IP y una puntuación del dominio (*rating*) que incluye la categoría FortiGuard asignada a la página web. Si la categoría FortiGuard está configurada para ser bloqueada, no se devuelve al peticionario el resultado de la petición DNS.

290. FortiGuard contiene una base de datos de direcciones conocidas de *Botnet* y servidores C&C (*Command and Control*). Esta base de datos se actualiza y se carga dinámicamente en FortiProxy, y está accesible si se dispone de la licencia de filtrado web de FortiGuard. Las peticiones DNS a una dirección de *Botnet* C&C son, utilizando los decodificadores IPS, examinadas contra la base de datos *Botnet* C&C y, si forma parte de la lista, se bloquean. Este bloqueo se habilita desde **Security Profiles > DNS Filter > Block DNS requests to known botnet C&C**. La base de datos actual que se está utilizando se puede visualizar desde **System > FortiGuard > Botnet Definitions**.

New DNS Filter Profile

Name

Comments 0/255

Redirect botnet C&C requests to Block Portal

43798 domains in botnet package

Enforce 'Safe Search' on Google, Bing, YouTube

FortiGuard Category Based Filter

Allow
 Monitor
 Redirect to Block Portal

Name	Action
Adult/Mature Content 15 15	
Alternative Beliefs	<input type="checkbox"/> Monitor
Abortion	<input type="checkbox"/> Monitor
Other Adult Materials	<input type="checkbox"/> Monitor
Advocacy Organizations	<input type="checkbox"/> Monitor
Gambling	<input type="checkbox"/> Monitor
Nudity and Risque	<input type="checkbox"/> Monitor
Pornography	<input type="checkbox"/> Monitor
Dating	<input type="checkbox"/> Monitor

0% **88**

Static Domain Filter

Domain Filter

External IP Block Lists

DNS Translation

Options

Redirect Portal IP

Allow DNS requests when a rating error occurs

Figura 31 – Configuración de Perfil de protección DNS

Entitlement	Status	
FortiCare Support	Registered	Actions
Virtual Machine	Valid (Expiration Date: 2022/09/16)	FortiProxy VM License
Firmware & General Updates	Licensed (Expiration Date: 2022/09/17)	
Intrusion Prevention	Licensed (Expiration Date: 2022/09/17)	Actions
IPS Definitions	Version 18.00184	
IPS Engine	Version 7.00029	
Malicious URLs	Version 3.00167	
Botnet IPs	Version 7.01958	View List
Botnet Domains	Version 2.00860	View List
AntiVirus	Licensed (Expiration Date: 2022/09/17)	
Web Filtering	Licensed (Expiration Date: 2022/09/17)	
Outbreak Prevention	Not Licensed	Purchase
FortiCloud Logs	Not Activated	Activate
Content Analysis	Licensed	

Figura 32 – Detalle de protección Anti-Botnet

291. El perfil de seguridad de filtrado DNS también dispone de filtros de URL (*static URL filters*) que permiten bloquear, eximir, permitir o monitorizar peticiones DNS utilizando IPS para examinar los paquetes DNS y ver si el dominio concuerda con alguno de los indicados en la lista de URLs.
292. El perfil de seguridad de Filtrado DNS se configura desde **Security Profiles > DNS Filter**. Se recomienda crear un perfil por defecto, que bloquee todas las peticiones DNS a *Botnet* y servidores C&C registrados en FortiGuard (opción *Block DNS requests to known botnet C&C*).
293. Para más información sobre la configuración de estos perfiles de seguridad, consultar el capítulo “*Security Profiles*” de *FortiProxy Administration Guide [REF2]*.

6.13 VPN

294. El dispositivo FortiProxy permite el establecimiento de Redes Privadas Virtuales basadas en los protocolos IPsec y SSL.
295. La funcionalidad VPN está integrada también en FortiClient, que permite el establecimiento de una VPN desde un equipo cliente (VPN acceso remoto). También es posible integrarlo a través de software de cliente VPN de terceros, de forma que este tráfico VPN pueda ser analizado por el módulo de firewall.
296. Además, se soportan VPNs con IPv6, ya sean *site-to-site* IPv6 sobre IPv6, IPv4 sobre IPv6 o IPv6 sobre IPv4, así como *Dynamic DNS*, de modo que aquellos equipos con direccionamiento IP dinámico puedan tener asignado un nombre DNS para poder estar siempre localizables. **No deberán utilizarse servicios externos de DNS dinámicos.**

6.13.1 VPN IPSEC

297. Una VPN basada en IPsec extiende una red privada a través de otra red pública, de modo que el tráfico intercambiado entre los extremos está cifrado y es

transparente para la red utilizada como transporte. Es necesario que los dos extremos de la VPN implementen el mismo protocolo. Por ello, se debe disponer de otro equipo FortiGate o de otro fabricante compatible, que actúe como el servidor VPN extremo (*VPN peer*), o un cliente VPN software (FortiClient) para PC o dispositivo móvil.

298. Debe existir una política de seguridad que permita el paso del tráfico entre la red privada y el túnel IPsec VPN. Esta política debe especificar el interfaz de la unidad FortiProxy que se conecta físicamente al servidor VPN remoto (*VPN peer*), el interfaz que se conecta a la red interna, la dirección IP origen de los datos que pasarán a través del túnel y, opcionalmente, restricciones temporales del uso la VPN y selección de aquellos servicios permitidos. La acción asociada con esta política será "IPsec", cifrando los datos hasta el otro extremo de la VPN y permitiendo el tráfico que haga "match" con los requisitos establecidos por la política.
299. Cuando una unidad FortiProxy recibe una petición de conexión de un VPN peer, utiliza los parámetros configurados para IPsec Fase 1 para establecer una primera conexión segura, así como autenticar al VPN peer e intercambiar información de autenticación. Una vez hecho esto, si existe una política de seguridad que permite la conexión, la unidad FortiProxy establece el túnel VPN con los parámetros configurados para IPsec Fase 2, y aplica la política de seguridad IPsec. Las claves de cifrado, autenticación y servicios de seguridad son negociados de forma dinámica entre los pares de la comunicación, a través del protocolo IKE.
300. Todas las VPN deberán configurarse de forma que se utilicen algoritmos de cifrado con una fortaleza criptológica de 128 bits o superior, de acuerdo a lo estipulado en la guía CCN-STIC-807 [REF3] para el ENS Categoría Alta.
301. La configuración del túnel se realiza desde **VPN > IPsec Tunnels**.

The screenshot shows the 'New VPN Tunnel' configuration page in FortiGate. It is divided into several sections: 'Network' (Remote Gateway, IP Address, Interface, Local Gateway, NAT Traversal, Keypair Frequency, Forward Error Correction), 'Authentication' (Method, Pre-shared Key, IKE Version, Mode), 'Phase 1 Proposal' (Encryption, Authentication, Diffie-Hellman Groups, Key Lifetime), 'XAUTH' (Type), 'Phase 2 Selectors' (Name, Local Address, Remote Address), and 'New Phase 2' (Name, Comments, Local Address, Remote Address, Subnet).

Figura 33 – Configuración de túnel VPN IPSEC

302. A continuación, se indican una serie de recomendaciones para configurar la Fase 1 de IPsec. Algunos parámetros corresponden a la configuración avanzada y solo se pueden configurar desde CLI:

- a) Seleccionar, si es posible, IKEv2 (solo disponible para VPN *route-based*, no para VPN *policy-based*). **IKEv1 se considera obsoleto y por lo tanto se desaconseja su uso.**

NOTA: No es posible forzar el uso exclusivo del protocolo IKEv2, y su aplicación recae en la responsabilidad de los operadores/administradores de la unidad FortiProxy.

- b) En el caso **excepcional** de que se utilice IKEv1 (en casos en que su uso sea imprescindible por cuestiones de compatibilidad con otras tecnologías), se debe seleccionar *Main Mode* (solo disponible en esta versión del protocolo). En el modo *Main Mode* los parámetros asociados a la Fase 1 son intercambiados en múltiples rondas, con información de autenticación cifrada.
- c) Método de Autenticación: se recomienda el uso de Certificados. Únicamente se recomienda el uso de claves precompartidas (*pre-shared keys*) cuando sea posible asegurar que han sido generadas con la entropía suficiente para aportar la fortaleza deseada (Ej.: para sistemas del ENS categoría Alta se exigen 128 bits) y se renueven en un período inferior a su “cripto período”. En este caso, los usuarios de la VPN deben obtener la clave precompartida de la persona encargada de gestionar el servidor VPN, y añadir dicha clave a la configuración de su cliente VPN. La clave debe estar compuesta por al menos 16 caracteres alfanuméricos aleatorios.
- d) Para la autenticación mediante certificados, debe seleccionarse “*Signatures*” en *Authentication Method*, y en *Certificate Name*, seleccionar el nombre del certificado que utilizará la unidad FortiProxy para la autenticación contra el otro VPN peer.
- e) La unidad FortiProxy debe tener instalado el certificado, así como el certificado raíz de la CA firmante del certificado del VPN peer (*root CA certificate*).
- f) Además, se recomienda utilizar el DN (*Distinguished Name*) del certificado que envía el VPN peer, para restringir el acceso únicamente a aquellos VPN peer que dispongan un DN específico. Para ello existen varias opciones de configuración.
- g) Una de ellas es cargar en la unidad FortiProxy el certificado del VPN peer, y al configurar la Fase 1, dentro de **Peer Options > Accept this peer certificate only**, seleccionar el nombre del certificado del VPN peer.
- h) Establecer un tiempo de inactividad del túnel (*IPsec tunnel idle timeout*) de forma que, transcurrido este tiempo, se cerrará la conexión de forma automática.

- i) Dentro de los parámetros criptográficos de *Phase 1 Proposal*, seleccionar aquellos que sean aceptados por la guía CCN-STIC-807 [REF3] para su uso en nivel Alto del ENS. En la siguiente tabla se muestra un resumen de los algoritmos criptográficos más habituales aceptados por esta guía, para los parámetros usados por FortiProxy. Es necesario indicar que en Modo FIPS, el producto no permite la selección de algoritmos considerados inseguros, como DES o 3DES, entre otros.

PARÁMETROS PHASE 1 Y 2 PROPOSAL	MÉTODOS Y ALGORITMOS AUTORIZADOS CCN-STIC-807
Protocolo IKE	IKEv2
Autenticación	SHA-256 o superior (SHA-384, SHA-512, etc.).
Grupo DH	DH Groups 15, 16, 19, 20, 21, 28, 29 o 30
Algoritmo de cifrado	AES en modo GCM y longitud de clave igual o superior a 128 bits

303. La Fase 1 solo se considera completada con éxito si se cumplen las siguientes condiciones:

- Cada “peer” de la comunicación negocia una política equivalente para el protocolo IKE.
- Cada peer está autenticado y sus identidades protegidas.
- Las claves pre-compartidas coinciden.

304. **A continuación, se indican una serie de recomendaciones para configurar la Fase2.**

En esta fase, los participantes en la comunicación negocian los algoritmos criptográficos que serán empleados durante el resto de la comunicación a través del túnel IPsec. Algunos parámetros corresponden a la configuración avanzada y solo se pueden configurar desde CLI (comando *config vpn phase2-interface*):

- Habilitar los parámetros: **Replay Detection y Perfect Forward Secrecy (PFS)**.
- Determinar un tiempo de vida de la clave de cifrado (en segundos o KB).
- Dentro de los parámetros criptográficos de Phase 2 Proposal, seleccionar aquellos que sean aceptados por la guía CCN-STIC-807[REF3] para su uso en nivel Alto del ENS (ver tabla anterior).
- Indicar que la fortaleza del cifrado de IPsec Fase 2 no debe exceder la de IKE Fase 1. Si se configura AES-128 para la Fase 1, la Fase 2 también debe usar AES-128. Si se configura AES-256 para la Fase 1, entonces la Fase 2 podría usar AES-128 o AES-256. **Se recomienda seleccionar el cifrado AES-256 en ambas fases.**

NOTA: “vpn phase2-interface” es como se denomina en la consola a la **Fase 2 del protocolo IPsec**.

305. La unidad FortiProxy permite monitorizar el uso de los túneles VPN IPsec, con la función de start/stop a disposición de los administradores. Esta monitorización se realiza desde la interfaz web, desde el menú **Monitor > IPsec Monitor**.
306. Es importante indicar que debe existir una política de seguridad que permita el paso de tráfico entre la red interna y el túnel VPN para que la comunicación se produzca.
307. Para más información sobre la configuración de las *VPN IPsec*, consultar *FortiOS Handbook (capítulo IPsec VPN)* [REF4].

6.13.2 VPN SSL

308. El usuario a través de un navegador web compatible, podrá también autenticarse y acceder a la red interna y aplicaciones de la organización a través de una VPN SSL.
309. Esto se configura desde **VPN > SSL-VPN Portals**, permitiendo tres modos: *tunnel-access* para acceder a la red interna en modo túnel, *web-access*, para acceder a un portal web que muestra solo aquellos recursos y aplicaciones (*bookmarks*) disponibles para ese usuario, y *full-access* que permite usar tanto el modo túnel como el modo web.
310. La funcionalidad de VPN SSL permite también chequear la postura de seguridad de los equipos de los usuarios (*host checking*). En conjunto con otras tecnologías como FortiNAC, FortiAuthenticator o FortiClient, será posible validar, entre otros, si el equipo ha iniciado sesión en el dominio, si tiene software con vulnerabilidades, etc. No obstante, teniendo únicamente en cuenta FortiProxy, el chequeo realizable es únicamente comprobar si posee antivirus.
311. A modo de ejemplo, se introducen los comandos necesarios para habilitar el host checking para comprobar el antivirus empleado en el equipo del usuario:

```
Config vpn ssl web portal
    Edit <nombre_regla>
        Set host-check av
    end
```

312. A continuación, se introduce el comando necesario para establecer un intervalo de tiempo entre operaciones de *host checking*. Tras la ejecución de este comando, se pedirá al usuario que indique un intervalo de tiempo entre 120 y 259200 segundos.

```
Set host-check-interval
```

313. Las conexiones de usuarios VPN SSL requieren un certificado para la autenticación de servidor, que deberá estar instalado en la unidad FortiProxy. Este certificado, por defecto, es auto firmado (*self-signed*). No obstante, **deberá instalarse un certificado X.509 emitido por una CA de confianza**. Tras instalar este certificado en la unidad FortiProxy, deberá ser seleccionado de la lista de *Server Certificates* desplegada en **VPN > SSL-VPN Settings**. En el cliente VPN SSL, deberá estar

instalado el certificado de la CA emisora (*root CA certificate*), y la lista CRL de dicha CA.

314. Respecto a la autenticación de cliente, FortiProxy proporciona varias opciones, desde la más simple a través de usuario y contraseña local, hasta la autenticación con un servidor LDAP, o autenticación a través de certificados.
315. Se recomienda configurar la autenticación de cliente por certificado, como un segundo factor de autenticación. Para ello, en **VPN > SSL-VPN Settings**, deberá seleccionarse *“Require Client Certificate”*. Además de disponer de un certificado instalado en el navegador del usuario VPN SSL, en la unidad FortiProxy deberá instalarse el certificado raíz de la CA emisora del certificado cliente (*root CA certificate*), y la lista CRL de dicha CA.
316. Para más información sobre la configuración de la autenticación de cliente por certificado, consultar el *FortiProxy Administration Guide*[REF2] capítulo *“Authentication – Certificate based authentication”*.

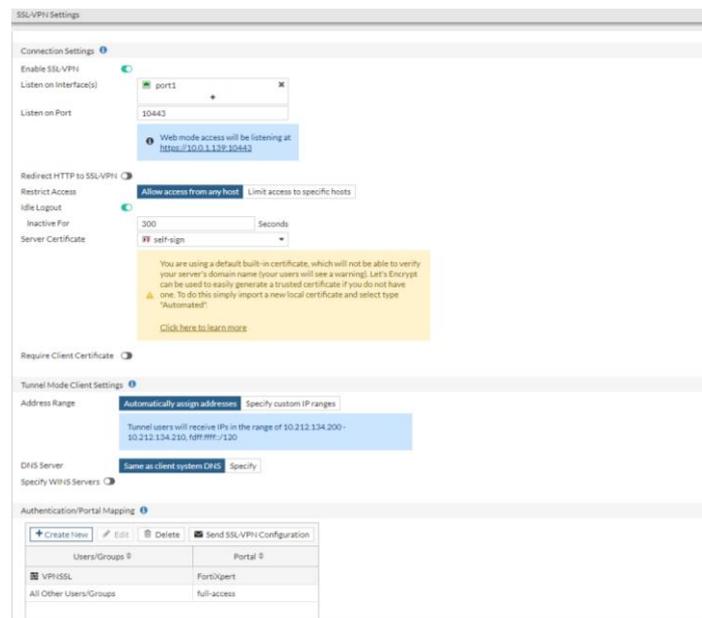


Figura 34– Configuración VPNSL

317. El detalle de la configuración de la VPN SSL se encuentra en el capítulo *“SSL VPN”* del FortiOS Handbook [REF4]. A continuación, se indican una serie de recomendaciones a tener en cuenta en la configuración de la VPN SSL (**VPN > SSL-VPN Settings**):

- Seleccionar el protocolo TLSv1.2 y deshabilitar el uso de TLS o SSL de versiones anteriores.
- Utilizar autenticación mutua a través de certificado en lugar de clave compartida.

- c) En la configuración de una VPN tipo túnel, no seleccionar *Split Tunneling*, para que todo el tráfico pase a través de la VPN.
- d) Especificar un *timeout* de autenticación, es decir, el tiempo máximo que un usuario podrá permanecer conectado hasta que el sistema le solicite de nuevo la autenticación. El rango en segundos de timeout de autenticación es de 0 a 259200 segundos.
- e) Especificar un *timeout* de inactividad, es decir, el tiempo máximo que se mantendrá la conexión inactiva, tras lo cual se producirá la desconexión automática. El rango de minutos de inactividad que se pueden establecer se sitúa entre 10 y 28800 segundos. Poner el valor a 0 implicaría deshabilitar la conexión por inactividad. Se recomienda establecer un *timeout* de inactividad de 300 segundos (5 minutos).
- f) A continuación, se enumera la secuencia de pasos necesarios para establecer un *timeout* de inactividad desde el GUI:
 1. Ir a **VPN > SSL-VPN Settings** y habilitar **Idle Logout**.
 2. En el campo **Inactive For**, introducir el valor de inactividad deseado.
 3. Seleccionar **Apply**.
- g) A continuación, se muestran los comandos necesarios para establecer un *timeout* de inactividad desde la consola (CLI).

```
Config vpn ssl settings
Set idle-timeout <seconds_int>
end
```

- h) Limitar a una, el número de conexiones VPN SSL simultáneas que podrá tener un mismo usuario. Habilitando esta opción, una vez que un usuario se ha logueado en el portal, las mismas credenciales no podrán ser empleadas en otro equipo para conectarse de forma simultánea.

318. Las conexiones VPN SSL activas se pueden monitorizar desde **User & Device > Monitor**. Se indica, para cada conexión activa, el nombre de usuario, IP del equipo conectado, y tiempo de inicio de la conexión. Existe la opción de finalizar cualquier conexión activa.

Refresh			
Username	Last Login	Remote Host	Active Connections
vpnuser1	2019/08/12 11:30:32	10.1.100.254	Tunnel: 20.2.200.1

Figura 35 – VPNSL User monitor

6.14 REGISTRO DE EVENTOS (LOGGING)

319. La función de registro de eventos o *logging*, registra todos los eventos relativos a las actividades de administración y gestión del dispositivo, las actividades del propio sistema, y todo el tráfico que pasa a través de la unidad FortiProxy, junto con las acciones que el dispositivo ha realizado durante su escaneado en función de las políticas y perfiles de seguridad definidos.

320. La información registrada genera un mensaje de log, que se almacena dentro de un fichero de log. Los ficheros de log siguen una nomenclatura en función del tipo de mensajes que almacenan, el dispositivo en el que se almacenan, la fecha/hora, y un ID identificativo, siguiendo el formato <logtype> - <logdevice> - <date> T <time>. <id>.log. Por ejemplo:

AntiVirusLog-disk-2019-09 13T11_07_57.922495.log.

- a) Existen los siguientes ficheros de log:
- **Tráfico.** Registra el tráfico que atraviesa el proxy a través de las políticas de seguridad, por lo que es referido como *Firewall Policy Logging*. Para ello, la política debe tener habilitada la opción de log.
 - **Eventos.** Registra todas las acciones realizadas en la gestión y administración del dispositivo, así como la actividad del sistema FortiProxy. Por ejemplo: modificaciones de la configuración, login de sesiones administrativas, eventos de Alta disponibilidad, etc.
 - **Antivirus, Web Filter, Application Control, Intrusion, Email Filter, Data Leak Prevention.** Registran las coincidencias (*match*) con las reglas configuradas en los correspondientes perfiles de seguridad. Para ello, los filtros y reglas de estos perfiles de seguridad deben tener la funcionalidad de auditoría habilitada, y deben estar asociados a las correspondientes políticas.

321. Cada política de seguridad debe tener habilitado el *logging* si se quiere tener registro del tráfico, tanto el permitido como el denegado. Las opciones de log en la política son:

- a) **Tráfico Admitido - No log** (*Log Allowed Traffic OFF*). No registra ningún mensaje de log sobre el tráfico permitido por la política.
- b) **Tráfico Admitido - Log de los eventos de seguridad** (*Log Allowed Traffic ON & Security Events ON*). Solo registra mensajes de log relacionados con eventos de seguridad que hayan sido causados por el tráfico permitido por la política.

- c) **Tráfico Admitido - Log de todas las sesiones** (*Log Allowed Traffic ON & All Sessions ON*). Registra todos los mensajes de log relativos a tráfico permitido por la política.



Figura 36 – Opciones de logging de tráfico en las políticas de Proxy

- d) **Tráfico Denegado – No Log** (*Log Violation Traffic OFF*). No registra el tráfico denegado.
- e) **Tráfico Denegado – Log** (*Log Violation Traffic ON*). Registra el tráfico denegado.

322. **Se recomienda habilitar en las políticas el logueo del tráfico admitido para todas las sesiones** (*Log Allowed Traffic ON & All Sessions ON*) y, en caso de que la política tenga asociados perfiles de seguridad (antivirus, IPS, filtrado web, etc.), habilitar también la opción de log en cada perfil de seguridad, para que quede registro de las coincidencias (*match*) encontradas por los filtros.

323. Es importante habilitar, también, el registro de todo el tráfico denegado por la política implícita por defecto del proxy mediante los comandos de CLI *“config log settings > set fwpolicy-implicit-log enable”*.

324. Hay que indicar que, en el modo de configuración seguro, el *logging* está habilitado por defecto para:

- Nuevas políticas de seguridad.
- Interfaces donde el acceso administrativo está habilitado.
- Intentos de conseguir acceso administrativo en interfaces donde el acceso administrativo no esté habilitado.
- Intentos fallidos de conexión a puertos TCP/IP distintos del 22 (SSH), 23 (telnet), 80 (HTTP), y 443 (HTTPS).
- Todos los cambios en la configuración.
- Fallos en la configuración.
- Conexiones bloqueadas por alcanzar el número máximo de intentos fallidos de autenticación.
- Revisión y visualización de los registros.

- i) Interfaces que se levantan(up) o se caen (down).
- j) Otro tráfico: paquetes ICMP descartados, paquetes IP inválidos descartados, inicios y cierres de sesión.
- k) Todos los tipos de eventos a partir del nivel de severidad “Información” (*Information severity level*).

325. Respecto al almacenamiento de los registros de log, FortiProxy permite:

- a) **Almacenamiento local en memoria del sistema o en disco duro.** El almacenamiento en memoria es el que está habilitado por defecto en el modo de operación seguro. La opción configurada cuando la memoria del sistema se llena, es la sobrescritura de los mensajes más antiguos. Todos los registros almacenados en memoria se borran cuando la unidad FortiProxy se reinicia. Los registros de auditoría almacenados en memoria son replicados en el disco duro del dispositivo. La información almacenada en la memoria del dispositivo se perderá en el momento del apagado del mismo.
- b) **Almacenamiento remoto,** enviando los registros a un servidor externo de auditoría a través de un canal seguro. FortiProxy soporta el uso de: FortiAnalyzer, FortiCloud, y Syslog.

326. Se recomienda el envío y almacenamiento de los registros de auditoría a un servidor externo.

6.14.1 FORTIANALYZER

327. FortiProxy se puede configurar para el envío automático de *logs* a FortiAnalyzer cada cierto tiempo configurable. Por defecto, los registros son cifrados en su envío a través de TLS 1.2. Es posible enviar *logs* simultáneamente a un máximo de 3 unidades FortiAnalyzer, permitiendo así una solución de *backup* para los registros.

328. Para conectarse a un dispositivo FortiAnalyzer funcionando en modo de operación seguro, es necesario instalar el certificado X.509 FortiAnalyzer en el equipo FortiProxy. La configuración se podrá realizar con los siguientes comandos CLI:

```
Config log fortianalyzer setting
    set status enable
    set server "IP_unidad FortiAnalyzer"
    set certificate "nombre_certificado"
    set upload-option realtime
end
```

329. En el ejemplo anterior, los *logs* se envían a FortiAnalyzer en tiempo real. También puede especificarse el envío diario, semanal o mensual. La configuración del envío automático de *logs* a FortiAnalyzer, se realiza también desde **Log & Report > Log**

Settings, habilitando “*Send Logs to FortiAnalyzer*”, bajo “*Remote Logging and Archiving*”.

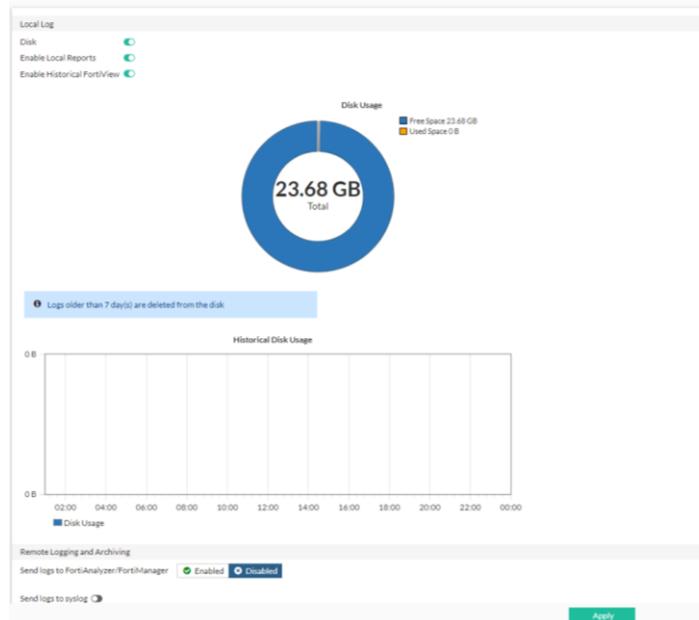


Figura 37 – Opciones de envío de log en FortiProxy

330. A continuación, se enumeran los pasos necesarios para programar el envío de *logs* de forma periódica a FortiAnalyzer.

- a) Ir a **Log & Reports > Log Settings**.
- b) En la sección **Remote Logging and Archiving**, seleccionar el recuadro asociado a **Send Logs to FortiAnalyzer/FortiManager**.
- c) Seleccionar **FortiAnalyzer (Daily at 00:00)**.
- d) Introducir la dirección IP de la unidad en el campo **IP Address**.
- e) Abrir el CLI para configurar la periodicidad de envío de logs.
- f) Introducir los siguientes comandos para configurar los períodos de envío:

```
Config log fortianalyzer setting
    Set upload-interval {daily | weekly |
    monthly}
    Set upload-time <hh:mm>
end
```

- g) Para cambiar el período de envío, en la interfaz gráfica (GUI), seleccionar **Change**, y hacer los cambios necesarios en la ventana **Upload Schedule**. A continuación, seleccionar **OK**.

331. Para más información sobre esta configuración, consultar *FortiOS Handbook* [REF4] capítulo “*Logging and Reporting*”.

332. En caso de que ocurra una interrupción en la comunicación entre los dispositivos FortiProxy y FortiAnalyzer, el administrador podrá reestablecer la conexión de forma manual enviando un *ping* al FortiAnalyzer desde la consola CLI de FortiProxy:

```
Exec ping <FortiAnalyzer IP address>
```

333. En caso de éxito, se reestablecerá la conexión entre los dos dispositivos. En caso contrario, esto significará que existe un problema en la red o en el equipo FortiAnalyzer.

6.14.2 SYSLOG

334. Las unidades FortiProxy también pueden enviar los registros a un servidor Syslog, soportando la característica de entrega fiable (*reliable delivery*) de Syslog, basada en la RFC 3195. Esta característica utiliza el protocolo TCP, garantizando la conexión fiable y la entrega de paquetes. Dentro de los perfiles de *reliable syslog*, FortiGate solo soporta el RAW. La característica *reliable syslog* está deshabilitada por defecto, y solo puede habilitarse a través de CLI, lo cual hace que FortiProxy modifique el puerto Syslog por defecto (514) al puerto TCP 601.

NOTA: Reliable Syslog es un estándar usado por TCP, empleado para garantizar la seguridad de la información intercambiada.

335. La configuración del envío de logs a un servidor Syslog, se lleva a cabo desde **Log & Report > Log Settings**. En caso de querer realizarse mediante CLI se deberá utilizar el comando:

```
Config log syslogd setting
```

336. Para más información sobre esta configuración, consultar *FortiOS Handbook* [REF4] capítulo “*Logging and Reporting*”.

7. FASE DE OPERACIÓN

337. Durante la fase de operación de la unidad FortiProxy, los administradores de seguridad deberán llevar a cabo, al menos, las siguientes tareas de mantenimiento:

- a) Comprobaciones periódicas del hardware y software para asegurar que no se ha introducido hardware o software no autorizado. El firmware activo y su integridad deberán verificarse periódicamente para comprobar que está libre de software malicioso.
- b) Aplicación regular de los parches de seguridad, con objeto de mantener una configuración segura.
- c) Mantenimiento de los registros de auditoría. Estos registros estarán protegidos de borrados y modificaciones no autorizadas, y solamente el personal de seguridad autorizado podrá acceder a ellos.
- d) La información de auditoría se guardará en las condiciones y por el periodo establecido en la normativa de seguridad.
- e) Auditar, al menos, los eventos especificados en la normativa de referencia y aquellos otros extraídos del análisis de riesgos.
- f) Actualización periódica de las bases de datos de firmas de amenazas conocidas.
- g) Realización periódica de copias de seguridad de las configuraciones del producto.

8. CHECKLIST

338. Para aplicar una configuración segura de Fortinet FortiProxy, se deberán realizar las siguientes acciones:

ACCIONES	SÍ	NO	OBSERVACIONES
INSTALACIÓN Y DESPLIEGUE			
Entrega segura del producto	<input type="checkbox"/>	<input type="checkbox"/>	
Creación de cuenta de soporte de Fortinet	<input type="checkbox"/>	<input type="checkbox"/>	
Registro del producto en la página web de soporte de Fortinet	<input type="checkbox"/>	<input type="checkbox"/>	
Descarga segura del firmware/software del producto	<input type="checkbox"/>	<input type="checkbox"/>	
Comprobación de la integridad del firmware/software descargado	<input type="checkbox"/>	<input type="checkbox"/>	
Activación de licencias	<input type="checkbox"/>	<input type="checkbox"/>	
Primer acceso al dispositivo y configuración inicial	<input type="checkbox"/>	<input type="checkbox"/>	
CONFIGURACIÓN			
Establecimiento del Modo de Operación Seguro	<input type="checkbox"/>	<input type="checkbox"/>	
Gestión de certificados	<input type="checkbox"/>	<input type="checkbox"/>	
Configuración de auto-chequeos	<input type="checkbox"/>	<input type="checkbox"/>	
Configuración de sincronización horaria (NTP)	<input type="checkbox"/>	<input type="checkbox"/>	
Activar los distintos módulos para cada grupo	<input type="checkbox"/>	<input type="checkbox"/>	
Revisión de eventos	<input type="checkbox"/>	<input type="checkbox"/>	
Configuración de backups	<input type="checkbox"/>	<input type="checkbox"/>	

9. REFERENCIAS

- REF1** FortiProxy 1.0 FIPS Level 2 Security Policy
<https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3628.pdf>
- REF2** FortiProxy Administration Guide 1.0.0
<https://docs.fortinet.com/product/fortiproxy/>
- REF3** FortiProxy CLI Reference 2.0.0
<https://docs.fortinet.com/document/fortiproxy/2.0.0/cli-reference>
- REF4** FortiOS Handbook
<https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/FortiOS-6.0-Handbook.pdf>
- REF5** Fortinet Support Website
<https://kb.fortinet.com/kb/microsites/microsite.do?cmd=displayKC&docType=kc%20&externalId=FD32312>
- REF6** Web Cache Communications Protocol (WCCP)
<https://datatracker.ietf.org/doc/html/draft-mclaggan-wccp-v2rev1-00>
- REF7** FIPS 140-2 Non-Proprietary Security Policy
<https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3628.pdf>

10.ABREVIATURAS

CCN	Centro Criptológico Nacional.
CPSTIC	Catálogo de productos y servicios de Seguridad TIC
DH	<i>Diffie – Hellman Algorithm</i>
DHCP	<i>Dynamic Host Configuration Protocol</i>
ECDSA	<i>Elliptic Curve Digital Signature Algorithm</i>
ENS	Esquema Nacional de Seguridad
FTP	<i>File Transport Protocol</i>
ICMP	<i>Internet Control Message Protocol</i>
IPS-CC	<i>Federal Information Processing Standard – Common Criteria</i>
IPsec	<i>Internet Protocol security</i>
RSA	Rivest, Shamir y Adleman <i>Algorithm</i>
SCP	<i>Secure Copy Protocol</i>
SHA	<i>Secure Hash Algorithm</i>
SSH	<i>Secure Shell Protocol</i>
SSL	<i>Secure Sockets Layer Protocol</i>
STIC	Seguridad de Tecnologías de Información y Comunicación
TCP	<i>Transmission Control Protocol</i>
TFTP	<i>Trivial File Transport Protocol</i>
TLS	<i>Transport Layer Security</i>
UDP	<i>User Datagram Protocol</i>
VPN	<i>Virtual Private Network</i>

