centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1406

Procedimiento de empleo seguro
Cortafuegos FortiGate

Abril de 2023

MINISTERIO DE DEFENSA

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2023.09.04 13:27:18 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-23-127-7.
Fecha de Edición: Abril de 2023

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

ÍNDICE

1. INTRODUCCIÓN

1. FortiGate NGFW *Appliances* son dispositivos diseñados para proporcionar servicios de *firewall* de nueva generación, asegurando la protección de redes IPv4 (*Internet Protocol version* 4) e IPv6 (*Internet Protocol version* 6).
2. Ofrecen un filtrado robusto basado en la información contenida en las cabeceras IPv4, IPv6, ICMPv4, ICMPv6, TCP y UDP. Adicionalmente, los dispositivos son capaces de realizar la inspección de contenido de los protocolos FTP, H.323, DCE-RPC, DNS y otros protocolos de naturaleza dinámica.
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 *customizadas*.
4. Los dispositivos emplean algoritmos y funciones criptográficas para la securización de las comunicaciones entre ellos mismos y las entidades a las que estén conectados. Esto incluye el servicio de Servidor o Gateway VPN para el establecimiento de túneles IPsec con otros servidores o clientes VPN, el servicio de Servidor VPN SSL para la conexión de usuarios, la administración remota a través de HTTPS, y el empleo del protocolo TLS hacia la plataforma de gestión de *logs* FortiAnalyzer.

2. OBJETO Y ALCANCE

5. En la presente guía se recoge el procedimiento de empleo seguro para las plataformas FortiGate que corren la versión 6.4 de FortiOS, para las funciones de cortafuegos y VPN-IPSEC.

3. ORGANIZACIÓN DEL DOCUMENTO

6. El presente documento se divide en las siguientes partes fundamentales, 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.

4. FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

7. 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 afectando así a 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 esté intacta y que no haya sido cortada ni se haya 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 esté 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.

8. 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.

9. La documentación enviada junto al dispositivo incluye una guía de inicio rápida, junto con un suplemento para el modelo hardware específico. El manual de FortiOS (***https://docs.fortinet.com/product/fortigate/6.4***) proporciona información detallada sobre los procesos de instalación y configuración del dispositivo y de todas sus funciones.

4.2 ENTORNO DE INSTALACIÓN SEGURO

10. Se recomienda instalar 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.

11. Para ello, la sala en la que se ubica el CPD debe estar 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 OPCIONES DE SOPORTE Y RMA FORTICARE

12. Se recomienda la contratación del servicio de soporte FortiCare para los equipos adquiridos, Fortinet ofrece dos (2) opciones de soporte según cada dispositivo adaptadas a las diferentes necesidades del organismo:

    a) *FortiCare Premium*

    b) *FortiCare Elite*. El servicio Elite proporciona tiempos de respuesta de 15 minutos para las familias de productos clave.

13. Existe la flexibilidad de adquirir diferentes niveles de servicio para diferentes dispositivos según sus necesidades de disponibilidad.

    https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-forticare-services.pdf

14. Además, Fortinet dispone de diferentes servicios de remplazo de quipo averiado "RMA" siendo siempre recomendada la opción "*Secure RMA*" cuando los equipos sobre los que se aplique tengan configuración y/o datos sensibles, ya que este sistema de RMA Seguro permite la ejecución de reemplazo del equipo averiado sin la necesidad de que este sea entregado.

    https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-forticare-technical-support-and-rma-services.pdf

4.4 REGISTRO DE LA UNIDAD

15. 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.

16. Para más detalles sobre el proceso de registro, acceder a *Fortinet Support Website Guide:*

    https://kb.fortinet.com/kb/microsites/microsite.do?cmd=displayKC&docType=kc&externalId=FD32312

4.5 CONSIDERACIONES PREVIAS

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

4.5.1 ENTROPÍA

18. Los modelos incluidos en la guía disponen de un chip FortiASIC CP9 de entropía integrado para proporcionar periódicamente la entropía al RGB.

4.5.2 MODO DE FUNCIONAMIENTO DEL CORTAFUEGOS

19. Los cortafuegos FortiGate pueden trabajar en modo enrutador (*NAT/Route Mode*) o en modo transparente (*Transparent Mode*).
20. 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*).
21. 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.
22. Para más información sobre la configuración del modo transparente, consultar *FortiOS Handbook*, capítulo "*Transparent Mode*":

    https://docs.fortinet.com/document/fortigate/6.4.12/administration-guide/302871/transparent-mode

4.5.3 USO DE DOMINIOS VIRTUALES (VDOMS)

23. Sobre una plataforma física se pueden utilizar hasta 500 dominios virtuales o VDOMs, independientes entre sí, con todas las funcionalidades de un dispositivo físico.
24. Si los requisitos de seguridad de un sistema implican la disposición de dos cortafuegos, nunca se puede considerar la utilización de dominios virtuales.
25. Se recomienda el uso de dominios virtuales (VDOMs) para segregar la administración y operación de cortafuegos, en aquellas arquitecturas que sólo requieran de un cortafuegos físico.

4.5.4 ENRUTAMIENTO

26. Los cortafuegos FortiGate soportan enrutamiento dinámico RIP (v1 y v2), OSPF (IPv4 e IPv6) y BGP v4, enrutamiento multicast PIM (*sparse mode y dense mode*), enrutamiento estático IPv6, y la posibilidad de hacer *policy routing*.

27. 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. Si no se recibe respuesta se considera la ruta caída, y comienza a utilizar una ruta alternativa.

28. Sólo se recomienda el uso de la funcionalidad *ping-server* o similar (tcp o udp echo), en redes donde el tráfico esté protegido con otras medidas adicionales (VPN o entornos aislados) y nunca en redes públicas, al tratarse de protocolos no seguros.

29. Cuando el *routing* se hace mediante rutas estáticas o rutas dinámicas usando OSPF y BGP, se pueden configurar múltiples rutas para un mismo destino, soportando redundancia entre ellas mediante el mecanismo ECMP (*Equal Cost Multi-path*), de tres (3) maneras posibles:

    a) ***source-ip-based***: se balancea el tráfico entre las distintas rutas de salida ECMP en función de las direcciones IP origen.

    b) ***weight-based***: se balancea el tráfico entre las distintas rutas de salida ECMP en función de los pesos establecidos en cada ruta estática de igual coste.

    c) ***usage-based***: se balancea el tráfico entre las distintas rutas de salida en función del porcentaje de uso de una interfaz. Una vez superado el porcentaje predefinido para una interfaz, comenzarán a utilizarse la ruta de salida ligada a otra interfaz.

30. Existe la funcionalidad de *policy-routing* para permitir el encaminamiento de los paquetes no solo en función del destino, si no también teniendo en cuenta el origen, el protocolo, el servicio o rango de puertos. Esto se configura desde el interfaz web: *Network > Policy Route*.

31. Si no son imprescindibles, se recomienda evitar los protocolos de enrutamiento dinámico, así como la posibilidad de *policy-based-routing*, toda vez que una debilidad en los protocolos de enrutamiento dinámico utilizados, puede ser explotada para desviar de manera maliciosa el tráfico, de la ruta prevista, y con ello sortear las medidas de seguridad diseñadas en la arquitectura de red. En este sentido, desde el punto de vista de seguridad, es preferible emplear únicamente rutas estáticas y nunca configurar una ruta por defecto.

32. Para más información sobre la configuración del enrutamiento consultar *FortiOS Handbook*, capítulo "*Advanced Routing*":

    https://docs.fortinet.com/document/fortigate/6.4.12/administration-guide/32143/advanced-routing

4.5.5 ALTA DISPONIBILIDAD

33. Es posible configurar un *cluster* para dotar al sistema de redundancia ante fallos. Se puede configurar activo-activo de modo que se balancee la carga, o 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.

34. Para proteger la integridad del dispositivo, así como las comunicaciones que soporta este, se recomienda considerar siempre el uso de soluciones basadas en *cluster*.

35. Un *cluster* activo-pasivo consiste en un equipo primario que procesa todo el tráfico, y uno o más equipos subordinados que están conectados a la red y al equipo primario, pero no procesan tráfico alguno. No obstante, los nodos secundarios pueden tener una copia de la tabla de sesiones si se habilita la opción "Enable Session Pick-up".

36. Para formar el *cluster*, los equipos de FortiGate utilizan un protocolo específico para la sincronización: FGCP (*Fortigate Cluster Protocol*).

37. El *cluster* puede estar formado por 4 dispositivos. Todos los equipos tienen que tener el mismo hardware y sistema operativo. Esta funcionalidad se soporta en modo enrutador y transparente.

38. 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 tanto de *firewall* como de VPN.

    c) Informar a los otros miembros del *cluster* del estado del equipo y sus enlaces.

39. Se recomienda que las interfaces empleadas para la transmisión del tráfico HA *heartbeat*, sean configuradas de modo redundante y dedicadas para proteger la integridad del *cluster*.

40. La configuración de alta disponibilidad se realiza desde el interfaz web: *System* > *HA*. Para más información consultar *FortiOS Handbook*, capítulo "*High Availability*":

    https://docs.fortinet.com/document/fortigate/6.4.12/administration-guide/666376/high-availability

4.5.6 OPTIMIZACIÓN WAN

41. 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 o MacroLans. Esta función está disponible por VDOM, configurándose de manera independiente para cada uno de ellos.

42. La tecnología de compresión utilizada es propiedad de Fortinet, con lo que no es compatible con aceleradores de terceros. Sí lo es con el cliente Forticlient WAN Optimization.

43. 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*, y la posible securización de la comunicación cliente/servidor a través de la red WAN gracias al establecimiento de un túnel seguro. Con esto se reducen latencias, se incrementa el rendimiento y se garantiza la privacidad en la comunicación.

44. Dicha tecnología requerirá el soporte en ambos extremos remotos, de la tecnología de optimización. Es decir, un sistema FortiGate (en modo NAT/*Route* o *Transparent*) o un *Forticlient* WAN *Optimization*. Es necesario que el sistema FortiGate tenga disco duro. Cuando sólo disponga de un disco duro, habrá que elegir si se usa para almacenar logs o para optimización WAN.

45. 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).

46. Para más información sobre la configuración del enrutamiento consultar FortiOS Handbook, capítulo “WAN Optimization, Web Cache, Explicit Proxy, and WCCP”.

4.5.7 AUTENTICACIÓN

47. A continuación, se indican los principales métodos de autenticación de usuarios o dispositivos, que puede utilizar la unidad FortiGate.

48. ***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. Esta autenticación puede ser local, cuando las credenciales se almacenan localmente en la unidad FortiGate, o puede utilizarse un servidor externo de autenticación.

49. El uso de servidores externos de autenticación es recomendable cuando varias unidades FortiGate deben autenticar a los mismos usuarios, o cuando una unidad FortiGate se añade a una red que ya dispone de servidores de autenticación. FortiGate soporta el uso de FortiAuthenticator, LDAP, RADIUS, TACACS+, SSO, AD o POP3.

50. Cuando se usa un servidor externo de autenticación, FortiGate 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.

51. La unidad FortiGate se deberá configurar para acceder al servidor externo. Esta configuración incluye los parámetros necesarios para autenticar a la unidad FortiGate contra el servidor de autenticación. La configuración se realiza a través del interfaz web: *User & Device > Authentication > RADIUS Servers / LDAP Servers / TACACS+ Servers, etc*.

52. ***Autenticación por certificado***. La unidad FortiGate 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.

53. ***Autenticación por claves pre-compartidas.*** Para el establecimiento de la VPN IPsec, la unidad FortiGate y el otro servidor VPN (*VPN peer*), o el cliente VPN, pueden autenticarse utilizando claves pre-compartidas (*preshared Keys*). La clave precompartida es una cadena de texto configurada en la unidad FortiGate y en el VPN peer o cliente, que se utilizará para cifrar los datos intercambiados para el establecimiento del túnel. Esta clave precompartida deberá ser distribuida a los dos peer de forma segura (*out of band*). **No se recomienda el uso de claves pre-compartidas para autenticación.**

54. ***Autenticación SSH por clave pública (SSH public key authentication).*** Para el establecimiento de conexiones SSH con la unidad FortiGate, se utilizarán parejas de claves pública-privada, de forma que la clave pública del cliente deberá estar instalada en el servidor y viceversa.

55. ***Autenticación por política de seguridad (Security Policy Authentication).*** Las políticas de seguridad controlan el flujo de tráfico entre redes. 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 certificado, a través de FSSO (*Fortinet Single Sign on*) o RADIUS SSO.

56. **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*). O en la autenticación del VPN *IPsec peer*, combinar el uso de certificado con el *peerID*.

57. Para más información sobre los métodos de autenticación, dirigirse al FortiOS *Handbook*, capítulo "*Authentication*".

5. FASE DE INSTALACIÓN

5.1 PRIMER ACCESO AL DISPOSITIVO

58. Para acceder al dispositivo por primera vez, se conectará el equipo del administrador al puerto de consola del equipo y, a través de un browser, se accede a la IP de la interfaz web por defecto del dispositivo (192.168.1.99), con el usuario por defecto *admin* y sin contraseña.

59. Se recomienda que, durante la fase instalación del equipo, este no esté conectado a Internet.

5.2 INSTALACIÓN DEL *FIRMWARE*

60. El primer paso en la instalación del dispositivo es la descarga e instalación del *firmware.*

61. Se recomienda la instalación de la versión 'segura' de *Firmware,* que es aquella que ha sido evaluada y dispone de la certificación Common Criteria: FortiGate FIPS-CC. 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 credencias obtenidas previamente durante el proceso de registro de la unidad.

    b) Ir a la página del *firmware,* seleccionar el firmware certificado **FortiGate 6.4** para el modelo hardware del dispositivo. Descargar el fichero de firmware en el equipo que usaremos para la instalación y anotar (se encuentra disponible en la misma página, junto al enlace de descarga) el valor de la firma de comprobación (checksum), disponible en formato SHA-512..

    c) Verificar la integridad del fichero de firmware descargado. Para ello, se calculará el checksum SHA-512 del fichero a través de alguna herramienta apropiada, y se comparará con el valor del checksum 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: *System > Status > System Information > Firmware Version*.

    d) Para la instalación del nuevo firmware usar la opción *Update*, seleccionando el fichero de firmware a instalar. La unidad FortiGate carga el archivo de

firmware, actualiza a la nueva versión, se reinicia y muestra el inicio de sesión de FortiGate. Este proceso toma unos pocos minutos.

e) Finalmente, comprobar que la versión de firmware instalada es la correcta.

62. Esta comprobación se puede realizar desde *System > Status > System Information*: hay una ventana con una consola abierta, al ejecutar el comando *get system status*.

63. En la documentación *FortiOS Cookbook* y *Handbook* se proporciona mayor detalle y otros métodos para la instalación del *firmware*.

5.3 ACCESO A BIOS

64. 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.

5.4 ENTROPÍA

65. La generación de claves de cifrado robustas requiere de una fuente de entropía robusta. Los modelos hardware a los que aplica la presente guía hacen uso de dos fuentes hardware de entropía: *FortiASIC CP9 o Fortinet Entropy Token.*

66. La fuente de entropía *FortiASIC CP9* va integrada en los modelos hardware de la serie E. Estos modelos usan esta fuente de entropía por defecto, sin necesidad de ningún tipo de configuración.

67. Para utilizar el *token* de entropía en el caso de FortiGate-VM sobre un hipervisor, como primera acción se deberá ligar el puerto USB que el *token* está utilizando, con la instancia de FortiGate-VM. Para ello, se deberán seguir los siguientes pasos:

```
Diagnose hardware lsusb
    BUS 006 Device 002 22a7:3001
    BUS 001 Device 001 1d6b:002 Linux Foundation 2.0 root hub
    BUS 002 Device 001 1d6b:002 Linux Foundation 2.0 root hub
    BUS 003 Device 001 1d6b:001 Linux Foundation 1.1 root hub
    BUS 004 Device 001 1d6b:001 Linux Foundation 1.1 root hub
```

68. Ejecutar el comando **diagnose hardware lsusb** en el hypervisor (FortiGypervisor-500D), e identificar el Bus y Device correspondientes al token (cuyo PID:VID es 22a7:3001).

69. Asignarle el *token* de entropía a la máquina virtual desde la consola delhypervisor:

```
config vm instance
  edit 1
    config usb
      set bus 6
      set device 2
    end
end
```

70. Como último paso, se deberá habilitar el *token* de entropía.

6. FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

71. El dispositivo debe operar en lo que se denominará **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.

72. 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.

73. El RBG 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).

74. Se recomienda configurar un periodo de realimentación de 60 minutos a través del parámetro *self-test-period*.

75. 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
  set self-test-period 60
end
```

76. 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***"

77. 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.

78. 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
```

79. 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 RNG seeding.***

80. Tras activar el modo de operación seguro:

    a) Todos los interfaces de red están desactivados (*down*) y no tienen dirección IP asignada. Esto incluye interfaces virtuales como el interfaz de la VPN SSL. 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 encuentran deshabilitados y no deben habilitarse:

        - Auto- instalación a través de USB.
        - Servidor local TFTP de la unidad FortiGate.
        - Comando **fnsysctl,** que proporciona acceso al sistema operativo subyacente.
        - Reportes de ataques de virus al servicio FortiGuard FDS (*FortiGuard Distribution Service*).

6.2 CERTIFICADOS

81. Se recomienda el uso de certificados en la unidad FortiGate, para la autenticación en las conexiones HTTPS de administradores, usuarios VPN SSL y pares VPN IPsec (*VPN peers*).

82. La unidad FortiGate 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 FortiGate permite generar un CSR (*Certificate Signing Request*) desde el interfaz web: *System > Certificates > Local Certificates > Generate*.

83. Opcionalmente, la unidad FortiGate permite la autenticación de clientes (usuarios administradores, usuarios VPN SSL y VPN IPsEC *peers*) a través de certificados, lo cual se recomienda, puesto que añade un segundo factor de autenticación. Para ello, en la unidad FortiGate, 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*.

84. Los certificados que se instalen en la unidad FortiGate 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 sobre el uso de algoritmos y funciones criptográficas en sistemas de categoría ALTA del ENS.

85. En *FortiOS Handbook* Capítulo "*Authentication – Certificate-based authentication*" se puede consultar más información sobre el uso de certificados.

6.3 ADMINISTRACIÓN DEL DISPOSITIVO

86. 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.

87. La administración segura de la unidad FortiGate 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*), 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:

```
config system interface
  edit <interfaz>
    set allowaccess https ssh
end
```

88. **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, a través de un protocolo seguro (HTTPS o SSH) con los comandos indicados anteriormente.

89. Se puede consultar más información sobre la configuración de administración del dispositivo en *FortiOS Handbook*, capítulo "*Getting Started – Basic Administration*":

    https://docs.fortinet.com/document/fortigate/6.4.12/administration-guide/383477/basic-administration

6.3.1 ADMINISTRACIÓN HTTPS (GUI)

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

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

92. 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 FortiGate, desde el interfaz web: System > Certificates > Import > CA Certificates, System > Certificates > Import > CRL.

    c) Crear una cuenta de usuario PKI para el administrador.

    d) Añadir la cuenta de usuario PKI al grupo de usuarios del cortafuegos dedicado a los administradores con autenticación PKI (PKI-authenticated administrators).

    e) En la configuración de la cuenta del administrador, seleccionar PKI como Tipo de cuenta y seleccionar como grupo de usuarios, aquel al que pertenece el administrador.

93. La unidad FortiGate soporta el uso de varias versiones de TLS. Deberá estar configurada para que haga uso de, como mínimo, la versión TLS 1.2, dado que versiones inferiores se consideran inseguras:

```
config system global
set admin-https-ssl-versions tlsv1-2
end
```

94. Para más información acerca del uso del interfaz web para la administración, consultar *FortiOS Handbook "Getting Started – Using the GUI":*

    https://docs.fortinet.com/document/fortigate/6.4.12/administration-guide/130914/using-the-gui

6.3.2 CONFIGURACIÓN DE SSH

95. Para la administración CLI a través de SSH, se recomienda configurar la autenticación mutua (cliente – unidad FortiGate), a través de claves públicas.

96. Para ello, se debe generar en el PC usado para la administración SSH, una pareja de claves pública – privada. La clave pública generada debe ser importada a la unidad FortiGate a través de los comandos:

```
config system admin
edit admin
        set ssh-public-key1 <key-type> <key-value>
end
```

97. Donde *<key-type>* debe ser "*ssh-dss*" 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 para el uso de algoritmos y funciones criptográficas en nivel alto del ENS.

98. Se recomienda, también, especificar el timeout máximo para autenticación (*login grace time*), 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

99. La autenticación por contraseña es un método efectivo únicamente si la contraseña es suficientemente robusta y se cambia periódicamente. Por defecto, la unidad FortiGate requiere únicamente que las contraseñas sean de, al menos, 9 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.

100. Para especificar la política de contraseñas desde el interfaz web de gestión: *System > Settings > Password Policy.*

101. Se recomienda especificar una política de contraseñas para la autenticación de administradores, con los siguientes requisitos mínimos:

    a) Longitud de la contraseña: mínimo 9 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) Cuando se cambia la contraseña, esta tendrá que diferir de la anterior en, al menos, las 5 contraseñas anteriores.

d) El cambio de contraseña debe realizarse cada cierto tiempo. Esto no puede ser forzado desde FortiGate y debe ser una práctica operativa (máximo 180 días, aunque se recomiendan tiempos menores para los administradores, ej.: 60 días).

e) Desde el cambio de contraseña, ésta no deberá ser cambiada en un mínimo de 4 días.

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.

102. Se puede consultar más información sobre la configuración de la política de contraseñas en *FortiOS Handbook*, capítulo "*Getting Started – Basic Administration*".

6.3.4 PARÁMETROS DE SESIÓN

103. A continuación, se indican una serie de recomendaciones para configurar diversos parámetros de sesión en las conexiones de los administradores a la unidad FortiGate:

a) **Timeout de autenticación:** 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*), no pueda ser utilizada de forma malintencionada durante largo periodo de tiempo.

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

b) **Limitar las sesiones concurrentes de un administrador**, de forma que solo haya una sesión activa (*admin-concurrent disable*).

c) **Limitar el número de administradores que pueden acceder simultáneamente a la unidad FortiGate** (*admin-login-max*).

d) **Timeout de inactividad para las conexiones de consola (admin-console-timeout) y para las conexiones remotas (admintimeout).** Transcurrido este tiempo con la sesión inactiva, se producirá la desconexión automática. De esta forma se evita que las sesiones de administración queden abiertas tras finalizar un trabajo.

e) **Número máximo de intentos fallidos de autenticación** (admin-lockout-threshold), y un **tiempo de espera tras superar un umbral** (admin-lockout-duration), evitando de esta manera ataques de fuerza bruta.

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 admintimeout 10
end
```

104. 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 FortiGate envía 300 caracteres de retorno de carro para limpiar la pantalla. Indicar que, 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"

105. 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.

106. Es imprescindible establecer la nueva contraseña robusta del usuario "admin", y restringir las direcciones IP origen desde las que puede acceder a la unidad FortiGate.

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

107. 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 fotitoken
    set fortitoken <NumerodeSerie>
  next
end
```

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

109. 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 deben utilizar usuarios nominales únicos para cada administrador y durante el tiempo estrictamente necesario.**

6.3.6 MENSAJE DE AVISO Y CONSENTIMIENTO

110. 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.

111. 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 global
  set pre-login-banner enable
end
```

112. 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 global
  set post-login-banner disable
end
```

113. 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

114. Los dispositivos FortiGate 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.

115. Debe impedirse el acceso a la configuración del dispositivo en el caso de tener acceso físico al dispositivo y no conocer las credenciales de administración. Se recomienda deshabilitar dicho usuario.

116. Para ello, ejecutar los siguientes comandos:

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

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

6.5 CONFIGURACIÓN DE INTERFACES

118. **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.

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

```
config system interface
edit "<interfaz>"
set status down
next
```

120. Desde la interfaz web, se puede deshabilitar los interfaces en *Network > Interfaces,* se edita el interfaz y, al final de las opciones, se encuentra la sección "*Status*", en la que se puede marcar *"Disabled"*.

121. 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.

122. 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>"
set alias "internet"
next
```

123. 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.

124. Finalmente, para evitar ataques de suplantación **se pueden configurar asociaciones de dirección IP y MAC para identificar las máquinas conectadas.** De este modo, solo se permitirá el acceso al tráfico recibido cuyas direcciones coincidan.

```
config firewall ipmacbinding table
edit <número de secuencia>
set ip <direccionip>
set mac <direccionMAC>
set name <nombre>
set status enable
```

125. 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.

126. A continuación, se realizan una serie de recomendaciones sobre servicios y protocolos:

a) 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*).

b) Deshabilitar cualquier mecanismo de detección de fallo de un interfaz, para evitar que pueda ser manipulado por un atacante y crear una denegación de servicio (*set fail-detect disable*).

c) No permitir el *fordwarding*, así como las redirecciones de cualquier protocolo (*set arpforward/ broadcast-forward/etc disable*).

d) Habilitar el envío de paquetes *TCP ident* a la configuración del interfaz

e) Implementar algún mecanismo de autenticación de red mediante portal cautivo (*set security-mode <captive>*).

f) No habilitar aquellos protocolos que difundan información sobre el dispositivo (*set device-identification / ipmac / etc. disable*).

127. Los comandos para realizar estas acciones, son los siguientes (consultar más información en *FortiOS CLI Reference)*.

```
config system interface
    edit "<interfaz>"
    set dhcp-relay-service disable
    set fail-detect disable
    set pptp-client disable
    set arpforward disable
    set broadcast-forward disable
    set l2forward disable
    set icmp-redirect disable
    set vlanforward disable
    set stpforward disable
    set ident-accept enable
    set ipmac disable
    set netbios-forward disable
    set security-mode <captive>
    set device-identification disable
    set lldp-transmision disable
    next
```

6.6 CONFIGURACIÓN DE SERVICIOS DEL DISPOSITIVO

128. 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.

129. A continuación, se realizan una serie de recomendaciones sobre ciertos servicios y protocolos:

a) Si no es necesario hacer redirecciones de tráfico, deshabilitar la redirección para evitar tener tráfico enrutado de vuelta por la misma interfaz.

b) Configurar la comprobación del número de secuencia de los paquetes TCP, así como *ICMP anti-replay.*

c) El número de entradas *arp* máximo configurado por defecto es 131.072, si no es suficiente se debe ajustar al valor adecuado a la red.

d) No extender el periodo de autenticación de la sesión para evitar el tiempo de *timeout*.

e) No permitir que pase tráfico sin escanear en situaciones de consumo excesivo de memoria.

f) Habilitar la comprobación de las cabeceras, así como de la correcta secuencia de los paquetes ESP, el SPI y su longitud. Del mismo modo, habilitar la comprobación de los paquetes de error ICMP.

g) Habilitar el control de acceso a los servidores *Fortiguard*.

h) Si no es necesario el controlador FortiExtender, deshabilitarlo.

i) Permitir la descarga del proceso IPSEC al hardware.

j) Si el dispositivo dispone de un display, requerir un PIN para su uso.

k) Deshabilitar el protocolo LLDP (*Link Layer Description Protocol*).

l) Habilitarse el timestamp de los mensajes de log.

m) Para evitar ataques de denegación de servicio, deshabilitar el envío de paquetes RESET a los originadores de sesiones TCP.

n) Por último, habilitar, mediante el motor IPS, la detección de ficheros con formato Hibun.

130. Los comandos para realizar estas acciones son los siguientes (consultar más información en FortiOS CLI *Reference*).

```
config system global
        set allow-traffic-redirect disable
        set anti-replay strict
        set arp-max-entry 131072
        set auth-keepalive disable
        set av-failopen off
        set av-failopen-session enable
        set check-protocol-header strict
        set check-reset-range strict
        set endpoint-control-fds-access enable
        set fds-statistics enable
        set fgd-alert-subscription advisory latest-threat
        set fortiextender disable
        set IPsec-hmac-offload enable
        set lcdpin <pin>
        set lcdprotection enable
        set lldp-transmission disable
        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 SINCRONIZACIÓN AUTOMÁTICA DEL RELOJ

131. Se debe 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.

132. Para ello, ejecutar los siguientes comandos:

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

133. Desde la interfaz web se puede configurar el reloj en *System > Settings > System Time*, aunque la totalidad de las opciones son únicamente accesibles mediante CLI.

6.8 *BACKUP* DE LA CONFIGURACIÓN

134. Una vez configurada la unidad FortiGate 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.

135. 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.

136. FortiGate 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).

137. 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 *Configuration > Backup*.

b) Seleccionar donde se almacenará el *Backup* (PC local o USB).

c) En caso de emplearse VDOMs, se deberá elegir entre realizar el backup únicamente de una VDOM específica (*VDOM Config*) o del dispositivo FortiGate entero (*Full Config*).

d) Seleccionar "*Encrypt configuration file*", esto pedirá introducir una contraseña, que será solicitada al restaurar el backup.

e) Seleccionar Backup. Se solicitará la ruta donde almacenar el fichero de backup (con extensión .conf).

138. Se recomienda proteger los ficheros de *backup* de la configuración de acuerdo a la política de seguridad correspondiente, y no emplear protocolos no seguros en la trasmisión de estos.

139. 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 *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*.

140. Además de la configuración, es recomendable guardar un backup de los certificados locales del dispositivo. Para exportar un certificado local y su clave privada en un fichero protegido PKCS12 a un servidor TFTP: ***execute vpn certificate local export tftp <cert_name> <filename> <tftp_ip>***

6.9 AUTO-CHEQUEOS

141. 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.

142. 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 **execute fips kat all**.

143. Para realizar un test de forma individual ejecutar **execute fips kat <test_name>**. En caso de querer visualizar una lista de los nombres de tests disponibles, **execute fips kat ?**.

144. En caso de que alguno de los test falle, el dispositivo FortiGate 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.

6.10 POLÍTICAS DE SEGURIDAD DEL CORTAFUEGOS

145. Los equipos FortiGate poseen la funcionalidad de cortafuegos basada en tecnología *Stateful Inspection Packet*. Esto le 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.

146. Las políticas de seguridad (***Security Policies***) o reglas del cortafuegos, controlan todo el tráfico que atraviesa el equipo. Se definen en base a los interfaces de entrada y salida, al origen (dirección IP, usuario o dispositivo) y a la dirección IP

destino. Permiten seleccionar, también, un rango temporal (*Schedule*) y un servicio o 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. Si no se encontrara ninguna regla que coincidiera con el paquete analizado, éste sería descartado (política de denegación implícita).

147. A la hora de configurar las reglas y políticas del cortafuegos, 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.

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

149. 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.

150. Se recomienda utilizar la variable *any* únicamente cuando esté debidamente justificado. Si no es necesario y se puede especificar el origen o destino, no se recomienda utilizar *any.*

151. Cuando se crea una política de seguridad estando el modo de operación seguro activado, por defecto esta no se encuentra habilitada, y deberá ser activada de forma explícita.

152. Se recomienda, al menos, crear las siguientes políticas en el cortafuegos (no están creadas por defecto):

a) Política de Bloqueo del tráfico local (direcciones desde 169.254.1.0 a 169.254.254.255).

b) Política de Bloqueo del tráfico de Clase E (240.0.0.0/24).

c) Política de restricción del espacio de direcciones IPv6 al espacio unicast asignado.

d) Políticas de protección DoS.

6.10.1 POLÍTICA DE BLOQUEO DEL TRÁFICO LOCAL

153. Para bloquear el tráfico local, se deberá crear una dirección del enlace local del cortafuegos y posteriormente crear las políticas para los interfaces que se quieren proteger. El siguiente ejemplo bloquea el tráfico con origen/destino el enlace local, desde la WAN a los interfaces internos:

```
config firewall address
        edit "Local-Link"
                set subnet 169.254.1.0  255.255.0.0
end
config firewall policy
        edit 1
                set srcintf "wan"
                set dstintf "internal"
                set srcaddr "Local-Link"
                set dstaddr "all"
                set action deny
                set status enable
                set schedule "always"
                set service "ALL"
        next
        edit 2
                set srcintf "wan"
                set dstintf "internal"
                set srcaddt "all"
                set dstaddr "Local-Link"
                set action deny
                set status enable
                set schedule "always"
                set service "ALL"
        next
end
```

6.10.2 POLÍTICA DE BLOQUEO DEL TRÁFICO DE CLASE E

154. Para bloquear el tráfico de clase E (*Class E*), se deberá crear una dirección de clase E en el cortafuegos y posteriormente crear las políticas para los interfaces que se quieren proteger. El siguiente ejemplo bloquea el tráfico de origen/destino de clase E desde la WAN a los interfaces internos:

```
config firewall address
        edit "Class-E"
                set subnet 240.0.0.0  240.0.0.0
end
config firewall policy
        edit 3
                set srcintf "internal"
                set dstintf "wan"
                set srcaddr "Class-E"
                set dstaddr "all"
                set action deny
                set status enable
                set schedule "always"
                set service "ALL"
        next
        edit 4
                set srcintf "wan"
                set dstintf "internal"
                set srcaddt "all"
                set dstaddt "Class-E"
                set action deny
                set status enable
                set schedule "always"
                set service "ALL"
        next
end
```

6.10.3 POLÍTICA DE RESTRICCIÓN IPV6

155. Para restringir el espacio de direcciones IPv6 al espacio global *unicast* asignado, se deberá crear una dirección IPv6 en el cortafuegos y posteriormente crear las políticas para los interfaces que se quieren proteger. El siguiente ejemplo bloquea el tráfico con origen/destino *unicast* global IPv6 desde la WAN, a las interfaces internas:

```
config firewall address6
        edit "IPv6-Global-Unicast"
                set ip6 2000::/3
        next
end
config firewall policy6
        edit 1
                set srcintf "wan"
                set dstintf "internal"
                set srcaddr "IPv6-Global-Unicast"
                set dstaddr "all"
                set action deny
                set status enable
                set schedule "always"
                set service "ALL"
                set srcaddr-negate enable
        next
        edit 2
                set srcintf "wan"
                set dstintf "internal"
                set srcaddt "all"
                set dstaddt "IPv6-Global-Unicast"
                set action deny
                set status enable
                set schedule "always"
                set service "ALL"
                set dstaddr-negate enable
        next
end
```

156. Es necesario tener en cuenta que este ejemplo cubre todo el rango *unicast* entero y bloqueará los intervalos especiales que podrían ser legítimos, incluidos todos los *Multicast* IPv6 (ff00 :: / 8), así como las direcciones reservadas para los mapeos *6to4* e *ipv4* (:: ffff: 0: 0/96, 4: ff9b :: / 96).

6.10.4 POLÍTICAS DE PROTECCIÓN DoS

157. Las políticas de protección DoS se configuran desde *Policy & Objects > DoS Policy*. Estas políticas solo afectan a los interfaces de entrada (*inbound*), y lo que hacen es inspeccionar el tráfico en busca de ciertos patrones y anomalías, relacionadas con comportamientos DoS. En caso de detectar tales anomalías, paralizan el tráfico con esos atributos.

158. Estas políticas disponen de múltiples anomalías predefinidas, como: Sync Flood, Port Scan, SRC session, icmp flood, udp flood, udp scan, etc.

159. Para más información sobre la configuración de las políticas del cortafuegos, consultar *FortiOS Handbook*, capítulo "*Firewall – Firewall Policies*".

6.11 PERFILES DE SEGURIDAD

160. Mientras que las políticas de seguridad del cortafuegos proporcionan las instrucciones al dispositivo para controlar el tráfico al que se permite pasar a través del cortafuegos, los perfiles de seguridad (***Security Profiles***) establecen los filtros que se deben aplicar al contenido del tráfico permitido por las políticas.

161. 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.

162. Los siguientes perfiles de seguridad están disponibles en FortiGate:

a) **Antivirus (AV)**. Es el perfil de seguridad que se utiliza para la protección contra la transimisión de código malicioso, referido normalmente como malware (troyanos, virus, gusanos, exploits de puerta trasera, spyware, radware, etc.)

b) **Filtrado Web (*Web Filtering*)**. Es el perfil de seguridad que se utiliza para proteger de URLs y contenidos web no apropiados.

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) **Filtrado *Anti-Spam***. Es el perfil que se utiliza para filtrar el tráfico de correo electrónico y evitar la entrada de spam o correos no deseados.

f) **DLP (*Data Leak Prevention*)**. Es el perfil que se utiliza para prevenir que información sensible pueda salir fuera de la red interna.

g) **FortiClient**. Es el perfil que se utiliza para forzar configuraciones de seguridad determinadas (protección antivirus, filtrado web, control de aplicaciones, etc.), en los endpoints que tengan instalado el software FortiClient.

h) **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.

163. Para poder utilizar estos perfiles, deben habilitarse estas características de seguridad desde *System* > *Feature Visibility*. Una vez activadas, se habilitará el perfil correspondiente en *Security Profiles*.

6.11.1 MODOS DE INSPECCIÓN

164. Los perfiles de seguridad que se definan para inspeccionar el tráfico asociado a una política de seguridad, pueden realizar la inspección en dos modos:

a) ***Proxy-Based***: este modo implica almancenar en un buffer el tráfico, y examinarlo de forma global antes de determinar la acción. El hecho de disponer de los datos completos permite examinarlos más en profundidad.

b) ***Flow-Based***: este modo inspecciona el tráfico según atraviesa el FortiGate, sin almancenarlo en ningún buffer. Según llega un paquete, este se inspecciona y se reenvía sin esperar al fichero o la página web completa.

165. *Flow-Based* es más eficiente, y el usuario aprecia una respuesta rápida a su petición, pero es menos seguro que *Proxy-Based* y puede generar más falsos positivos o falsos negativos al realizar una inspección menos profunda.

166. No todos los perfiles de seguridad están disponibles en ambos modos, como se muestra en la siguiente tabla:

PERFIL DE PROTECCIÓN	INSPECCIÓN BASADA EN FLUJO	INSPECCIÓN BASADA EN PROXY
FortiClient Profiles	x	x
AntiVirus	x	x
Web Filter	x	x
DNS Filter	x	x
Application Control	x	x
Intrusion Protection	x	x
Anti-Spam		x
Data Leak Protection		x
Proxy Options		x
SSL Inspection	x	x
SSH Inspection		x
VoIP/ICAP		x
Web Application Firewall		x
Web Rating Overrides	x	x
Web Profile Overrides		x

167. Desde el panel de información del sistema (*System Information dashboard widget*), se puede habilitar uno u otro modo de inspección. Cuando se habilita el modo *Flow-Based*, por ejemplo, todos los perfiles de seguridad que estaban en modo *Proxy-Based* se cambian al modo *Flow-Based*, y aquellos que solo están disponibles en modo *Proxy*, desaparecen del panel de configuración GUI.

168. El modo *Proxy-based* permite implementar funcionalidades de seguridad adicionales, como se refleja en la tabla anterior, aunque el modo *Flow-based*, por su diseño, proporciona igualmente una alta capacidad de securización junto a un mayor rendimiento.

169. En el modo *Proxy-based*, no obstante, se pueden configurar ciertas opciones para mitigar el retardo que puede producir este tipo de inspección. Estas opciones están disponibles desde el interfaz web: *Security Profiles > Proxy Options.* Algunas de ellas son las siguientes:

a) ***Confort Clients***. Permite, mientras se realiza la inspección de un fichero que el usuario ha solicitado descargar, enviarle un goteo de datos para que este compruebe que el fichero está en descarga. Sin embargo, estos datos que se envían no son escaneados, y pueden, por lo tanto, contener infecciones. Se recomienda no utilizar *Client Confort* y, en caso de que sea necesario, configurar un intervalo elevado y una cantidad de datos reducida.

b) ***Oversized Files***. Los ficheros descargados, en algunos casos, pueden ser de tamaños muy elevados (Kb o Gb). En estos casos, cuando el modo de inspección es *Proxy-Based* la unidad FortiGate puede no tener tamaño suficiente de memoria para realizar el *buffering* del fichero para su inspección. Para estos casos, la opción de *Block Oversized File/Email* permite, o bien bloquear, o bien admitir (sin escaneo) los ficheros que superen el tamaño configurado. Se recomienda el uso de esta opción con la acción de Bloqueo ya que, aunque la mayor parte de los ataques se producen a través de ficheros de tamaños muy reducidos, es arriesgado no inspeccionar el contenido de los ficheros grandes.

6.11.2 ANTIVIRUS

170. 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*).

171. En el perfil de AV se puede configurar que la unidad FortiGate aplique la protección antivirus a las sesiones HTTP, FTP, IMAP, POP3, SMTP, y NNTP. 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.

172. 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 FortiGate determina que el fichero ha sido infectado y toma la acción configurada en el perfil AV.

173. Todas las unidades FortiGate disponen de la base de datos de firmas *Normal*. Algunos modelos, además, disponen de otras dos BD: *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.

174. 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.

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

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

176. 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 sitos *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*.

177. Otra funcionalidad que se puede incorporar en el perfil de seguridad AV es la inspección de ficheros sospechosos, en FortiSandbox. Cuando FortiGate 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 FortiGate.

178. 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.

179. 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 FortiGate 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 *update now* desde la consola de gestión.

180. En entornos con alto nivel de seguridad puede no ser posible tener acceso a una red pública, para lo cual se deberán implementar soluciones para la actualización de la base de datos sin conexión directa. En este sentido, FortiManager puede actuar como nodo para los equipos que gestiona, sin que tengan acceso a la red pública.

181. La configuración del perfil de seguridad AV se realiza desde *Security Profiles* > *AntiVirus*. Se recomienda disponer de un perfil de seguridad AV por defecto, con el modo de inspección *Proxy-Based*, que boquee todos los virus detectados para todos los protocolos y, en caso de disponer del servicio, envíe todos los ficheros a FortiSandbox para inspección.

182. Para más información sobre la configuración de estos perfiles de seguridad, consultar el capítulo "*Security Profiles*" de *FortiOS Handbook*.

6.11.3 FILTRADO WEB

183. El perfil de seguridad de Filtrado Web (***Web Filter***) realiza el filtrado del tráfico HTTP. 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.

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

1. Filtrado URL.
2. Filtrado en función de las categorías FortiGuard.
3. Filtrado de Contenidos y Scripts web.
4. Escaneo antivirus.

185. 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 listas blancas frente a listas negras.**

186. 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 no solo permite el acceso a la URL, sino que no aplica ningún otro escaneo al tráfico. **No se recomienda el uso de la acción Eximir. Se recomienda utilizar, en su lugar, la acción Monitorizar.**

187. 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 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.

188. 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.

189. La configuración de los perfiles de Filtrado Web se realizar 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.

190. Para más información sobre la configuración de estos perfiles de seguridad, consultar el capítulo "*Security Profiles*" de *FortiOS Handbook*.

6.11.4 CONTROL DE APLICACIONES

191. El perfil de seguridad de Control de Aplicaciones (***Application Control***), permite que FortiGate 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 FortiGate, que pueden analizar el tráfico para detectar el que corresponde a determinadas aplicaciones, incluso aunque no utilicen puertos y protocolos estándar.

192. La unidad FortiGate 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.

193. La base de datos de firmas de aplicaciones que tiene la unidad FortiGate, 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*).

194. 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).

195. 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 con modo de inspección *Proxy-Based*, que bloquee todas las aplicaciones, excepto esas.

196. Para más información sobre la configuración de estos perfiles de seguridad, consultar el capítulo "*Security Profiles*" de *FortiOS Handbook*.

6.11.5 PROTECCIÓN DE INTRUSIONES (IPS)

197. A través de los perfiles de seguridad de IPS (***Intrusión Protection***), FortiGate 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 FortiGate o cualquier firma adicional que hayamos creado, se puede ver en *Security Profiles > Intrusion Protection > View IPS Signatures*.

198. 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, FortiGate buscará la firma del ataque únicamente en el tráfico que corresponda a ese protocolo.

199. La definición de las firmas que se van a buscar en determinado tráfico, se realiza a través de los Sensores IPS. 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:

a) **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).

b) **Basadas en puntuación (*Rate Based*)**. En la base de datos de firmas, suelen existir unas firmas por defecto con la acción asociada de Monitor. Estas son firmas de ataques que solo se consideran una amenaza importante si vienen en multitud.

c) **Customizadas**. Especificación manual.

200. 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).

201. Se puede habilitar en los filtros la opción de *Packet Logging*, para que FortiGate 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.

202. 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.*

203. En entornos con alto nivel de seguridad puede no ser posible tener acceso a una red pública, para lo cual se deberán implementar soluciones para la actualización de la base de datos sin conexión directa. En este sentido, FortiManager puede actuar como nodo para los equipos que gestiona, sin que tengan acceso a la red pública.

204. El perfil de seguridad de IPS se configura desde *Security Profiles > Intrusion Protection*. Se recomienda crear un perfil por defecto con modo de inspección *Proxy-Based*, que bloquee todo el tráfico que coincida con las firmas de los filtros configuradas, e ir permitiendo progresivamente aquellas firmas que generen falsos positivos.

205. Para más información sobre la configuración de estos perfiles de seguridad, consultar el capítulo "*Security Profiles*" de *FortiOS Handbook*.

6.11.6 FILTRADO *ANTI-SPAM*

206. El servicio ***Anti-Spam*** de FortiGate permite filtrar los correos IMAP, POP3 y SMTP y, en caso de que el modelo FortiGate disponga de la función de inspección SSL, también IMAPS, POP3S, y SMTPS, para detectar *spam* o palabras y ficheros no deseados dentro de los correos electrónicos.

207. Este filtrado solo es posible en el modo de inspección *Proxy-Based*.

208. Las técnicas *Anti-Spam* que puede usar la unidad FortiGate de forma local, son:

a) Listas blancas y negras de direcciones IP y direcciones de correo, permitiendo usar comodines y expresiones regulares.

b) **Listas de palabras prohibidas (*banned words*)** dentro de los mensajes de correo, de forma que se considere como *spam* en caso de superar un umbral configurable.

209. También se puede utilizar el servicio *Anti-Spam* de FortiGuard, que dispone de bases de datos de reputación de IPs y de firmas de *spam*, junto con filtros más avanzados de detección. Utilizando el servicio de filtrado *Anti-Spam* de FortiGuard, se puede filtrar utilizando chequeos de direcciones IP, de URLs, de *checksum* de correos, detectar URLs de *phishing* en correos, etc.

210. Tan pronto como alguno de los filtros aplicados identifica el mensaje como *spam*, se procede a realizar la acción definida para cada filtro, que podrá ser:

a) ***Tag***: el mensaje quedará marcado en algún sitio como Spam, de forma que el receptor pueda identificarlo.

b) ***Pass***: no se realiza ningún filtrado para el protocolo especificado.

c) ***Discard* (solo para SMTP/SMTPS)**: el mensaje es descartado sin enviar ninguna notificación a emisor ni a receptor.

211. El perfil de seguridad *Anti-Spam* se configura desde *Security Profiles > Anti-Spam*. Es conveniente habilitar la detección y filtrado de tráfico *spam*, independientemente de que tengamos una solución en nuestra red para ello. Por ello, se recomienda crear un perfil *Anti-Spam* por defecto con modo de inspección *Proxy-Based*, que detecte y marque como *spam* los correos detectados. Si existe la posibilidad de saber las direcciones IP de los servidores de correo con los que vamos a tener tráfico, se recomienda crear una lista blanca para permitir el tráfico de correo electrónico únicamente con esos servidores.

212. Para más información sobre la configuración de estos perfiles de seguridad, consultar el capítulo "*Security Profiles*" de *FortiOS Handbook*.

6.11.7 DLP

213. La característica de Prevención de Fuga de Información o ***DLP*** (***Data Leak Prevention***) permite filtrar los datos que pasan a través de la unidad FortiGate, 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 FortiGate, serán detectados y bloqueados, o permitidos y registrados (*logged*).

214. Este filtrado solo es posible en el modo de inspección *Proxy-Based*.

215. 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).

216. La unidad FortiGate 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.

217. 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 FortiGate que disponen de espacio de almacenamiento).

218. 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 FortiGate 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.

219. El perfil de seguridad de DLP se configura desde *Security Profiles > Data Leak* Prevention. Se recomienda crear un perfil por defecto con modo de inspección *Proxy-Based*, que bloquee cualquier tráfico relacionado con información que tengamos clasificada como no pública.

220. Para más información sobre la configuración de estos perfiles de seguridad, consultar el capítulo "*Security Profiles*" de *FortiOS Handbook*.

6.11.8 INSPECCIÓN DEL TRÁFICO SSH/SSL

221. FortiGate permite la creación de perfiles para la inspección del tráfico SSH/SSL. Esta inspección permite aplicar escaneado antivirus, filtrado web, y filtrado *anti-spam* al tráfico cifrado. Para ello, la unidad FortiGate:

a) Intercepta y descifra las sesiones HTTPS, IMAPS, POP3S, SMTPS, y FTPS entre clientes y servidores.

b) Aplica la inspeción de contenido a los datos descifrados, incluyendo 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.

222. 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 FortiGate tiene 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 FortiGate.

223. 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, no los contenidos del tráfico.

224. 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 customizados para servidores SSL específicos con un certificado específico.

225. A la hora de crear un perfil de inspección SSL, debe seleccionarse el certificado que va a utilizar la unidad FortiGate. Puede ser 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), o puede ser un certificado auto-firmado (*self-signed*), en cuyo caso será necesario desplegarlo en todos los clientes para no generar errores de certificado.

226. 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 filtrados antivirus, DLP, filtrado Web y Anti-Spam.

227. Para más información sobre la configuración de estos perfiles de seguridad, consultar el capítulo "*Security Profiles*" de *FortiOS Handbook*.

6.11.9 PROTECCIÓN DEL *ENDPOINT* (FORTICLIENT)

228. La protección del *endpoint* se basa en que esté instalada y actualizada, la aplicación ***FortiClient*** en los *endpoints*. A través del perfil de seguridad FortiClient, la unidad FortiGate establece una configuración de seguridad en todos los clientes desplegados que, entre otros parámetros, obligará a:

a) Protección antivirus en tiempo real.

b) Filtrado desde FortiClient de categorías web, basado en los filtros web definidos en FortiGate.

c) Control de aplicaciones desde FortiClient, basado en los sensores de aplicación definidos en FortiGate.

229. Es posible forzar la instalación y uso de FortiClient en los *endpoints*. De esta forma, cuando un usuario abre un navegador web, FortiGate le devolverá un mensaje indicando que debe instalar FortiClient, junto con el enlace para la instalación. El usuario no podrá continuar hasta que realice la instalación del cliente. Una vez instalado, FortiGate enviará un mensaje al usuario para que se registre en la unidad FortiGate. Una vez registrado, FortiGate envía el perfil de seguridad FortiClient al software FortiClient del *endpoint*. A partir de ahí el usuario ya podrá conectarse a la red.

230. Para forzar el uso de FortiClient, la unidad FortiGate debe tener habilitado el registro de los *endpoints*, habilitando la opción de *FortiHeartBeat* en la interfaz correspondiente. Los dispositivos que se conecten a ese interfaz serán forzados a registrarse en FortiGate e instalar FortiClient antes de conseguir acceso a los servicios de red.

231. Se recomienda forzar el registro y uso de FortiClient en todos los *endpoints* desplegados, así como la creación de perfiles FortiClient para todos los clientes (*Security Profiles > FortiClient Profiles*), con las siguientes opciones habilitadas:

a) Protección Antivirus, incluyendo Scan File Downloads, Block malicious websites, y Block attack channels.

b) Filtrado Web, asignando los filtros web apropiados, que deben haberse creado previamente (*Security Profiles > Web Filtering*).

c) Control de aplicaciones, asignando los sensores de aplicación apropiados, que deben haberse creado previamente (*Security Profiles > Application Control*).

232. Para más información sobre la configuración de estos perfiles de seguridad, consultar el capítulo "*Security Profiles*" de *FortiOS Handbook*.

6.11.10 FILTRADO DNS

233. 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 FortiGate 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 (*raiting*) 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.

234. FortiGuard contiene una nueva 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 FortiGate, 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.*

235. 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.

236. El perfil de seguridad de filtrado DNS y la protección Botnet están disponibles tanto en el modo de inspección *Proxy-Based*, como en el modo *Flow-Based.*

237. El perfil de seguridad de Filtrado DNS se configura desde *Security Profiles > DNS Filter*. Se recomienda crear un perfil por defecto con modo de inspección *Proxy-Based*, que bloquee todas las peticiones DNS a *Botnet* y servidores C&C registrados en FortiGuard (opción *Block DNS requests to known botnet C&C*).

238. Para más información sobre la configuración de estos perfiles de seguridad, consultar el capítulo "*Security Profiles*" de *FortiOS Handbook*.

6.12 *PROXY* EXPLÍCITO

239. Si no se dispone de servidor *proxy* en la red de la organización, la unidad FortiGate tiene la capacidad de ofrecer el servicio de Proxy web explícito (*Explicit Web Proxy*) para el tráfico HTTP y HTTPS en uno o más interfaces de FortiGate. El proxy web soporta, también, la función de proxy para sesiones FTP, y la función de autoconfiguración *proxy* (PAC) para proporcionar configuraciones del proxy automáticas a los usuarios del proxy explícito.

240. Esta característica, debe habilitarse en System > Feature Visibility> Explicit Proxy, y en Network > Explicit Proxy > Explicit Web Proxy.

241. Para permitir explícitamente el tráfico web del proxy que va a atravesar el FortiGate, debe crearse la correspondiente política de seguridad que lo permita, de forma que podrán también aplicarse perfiles de seguridad, como el escaneo antivirus, filtrado

web, control de aplicaciones, etc. **Deberá dejarse la política de *proxy* web por defecto a Bloqueo (*Deny*), e ir añadiendo políticas de *proxy* web específicas**.

242. Deben añadirse los interfaces del proxy explícito desde *Network > Interfaces*, editando el interfaz y habilitando la opción de *Explicit Web Proxy*. En *Policy & Objects > Addresses* se debe añadir una dirección del cortafuegos que concuerde con la dirección origen de los paquetes que serán aceptados por el proxy. Finalmente, debe crearse la política de seguridad desde *Policy & Object > Proxy Policy* para aceptar el tráfico para el que se permita el uso del proxy explícito.

243. El tráfico que no es aceptado por la política configurada, puede ser descartado o admitido, dependiendo de la acción por defecto (*Default Firewall Policy Action*) que se haya configurado en *Network > Explicit Proxy*. Se recomienda que la acción por defecto sea Denegar (*Deny*), ya que en caso de que sea permitir (*Allow*), el tráfico que no es aceptado por la política de seguridad sería permitido sin restricciones o procesamientos adicionales.

244. Para utilizar el proxy explícito, los usuarios deben añadir en la configuración proxy de sus navegadores la dirección IP del interfaz de FortiGate donde está habilitado el proxy, y el número de puerto del proxy web (8080 por defecto).

245. Es imprescindible disponer de un servicio de proxy para el tráfico HTTP, ya sea en un equipo dedicado, o a través del cortafuegos. Además, hay que asegurar que todo el tráfico hacia redes externas pasa a través del mismo.

246. Para más información sobre la configuración del proxy explícito, consultar el capítulo "*WAN Optimization, Web Cache, Explicit Proxy, and WCCP*" de FortiOS *Handbook*.

6.13 VPN

247. El dispositivo FortiGate permite el establecimiento de Redes Privadas Virtuales basadas en protocolos IPSec y SSL.

248. 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.

249. 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

250. 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, debemos 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.

251. 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 FortiGate 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", lo que permitirá configurar todos los parámetros del túnel VPN.

252. Cuando una unidad FortiGate recibe una petición de conexión de un VPN peer, utiliza los parámetros configurados para IPsec Fase 1 para establecer una primera conexión segura y autenticar al VPN peer. Una vez hecho esto, si existe la política de seguridad que permite la conexión, la unidad FortiGate 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 peer, a través del protocolo IKE.

253. 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 para el ENS Categoría Alta.

254. La configuración del túnel se realiza desde *VPN > IPsec Tunnels*.

255. **A continuación, se indican una serie de recomendaciones para configurar la Fase1.** 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.

b) En el caso excepcional de que se utilice IKEv1 se debe seleccionar *Main Mode* (solo disponible en esta versión del protocolo).

c) Método de Autenticación: se recomienda el uso de Certificados. Únicamente se recomienda el uso de claves precompartidas (*pre-shared keys*) cuando sea posible determinar que posee la fortaleza exigida

d) Para ello, debe seleccionarse "*Signatures*" en *Authentication Method*, y en *Certificate Name*, seleccionar el nombre del certificado que utilizará la unidad FortiGate para la autenticación contra el otro VPN peer.

e) La unidad FortiGate 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, una de ellas es cargar en la unidad FortiGate 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.

g) En el caso de que el VPN Peer sea otra unidad FortiGate se recomienda, además, añadir in ID que FortiGate comprobará para aceptar la conexión. Este ID del VPN peer se configura en *Phase 1 Proposal > Peer Options > This peer ID*. En la unidad FortiGate que representa el VPN peer, el ID que enviará a nuestra unidad FortiGate se configura en *Phase 1 Proposal > Advanced > Local ID.*

h) Establecer un tiempo de inactividad del túnel (*IPsec tunel 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 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 FortiGate.

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 CBC o GCM y longitud de clave igual o superior a 128 bits

256. **A continuación, se indican una serie de recomendaciones para configurar la Fase2**. Algunos parámetros corresponden a la configuración avanzada y solo se pueden configurar desde CLI:

a) Habilitar los parámetros: Replay detection y Perfect forward secrecy (PFS).

b) Determinar un tiempo de vida de la clave de cifrado (en segundos o KB).

c) Dentro de los parámetros critográficos de *Phase 2 Proposal*, seleccionar aquellos que sean aceptados por la guía CCN-STIC-807 para su uso en nivel Alto del ENS (ver tabla anterior).

d) 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 cofigura 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.**

257. La unidad FortiGate 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 *Monitor > IPsec Monitor*.

258. Para más información sobre la configuración de las *VPN IPsec*, consultar *FortiOS Handbook (capítulo IPsec VPN)*.

6.13.2 VPN SSL

259. 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.

260. 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.

261. La funcionalidad de VPN SSL permite también chequear la postura de seguridad de los equipos de los usuarios (*host checking*).

262. Las conexiones de usuarios VPN SSL requieren un certificado para la autenticación de servidor, que deberá estar instalado en la unidad FortiGate. 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 FortiGate, 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.

263. Respecto a la autenticación de cliente, FortiGate 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.

264. 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 FortiGate deberá instalarse el certificado raíz de la CA emisora del certificado cliente (*root CA certificate*), y la lista CRL de dicha CA.

265. Para más información sobre la configuración de la autenticación de cliente por certificado, consultar el *FortiGate Handbook* capítulo "*Authentication – Certificate based authentication*".

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

a) Seleccionar el protocolo TLS 1.2 y deshabilitar el uso de TLS o SSL de versiones anteriores.

b) Utilizar autenticación mútua a través de certificado como se ha comentado anteriormente.

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.

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.

f) Limitar a una, el número de conexiones VPN SSL simultáneas que podrá tener un mismo usuario.

267. 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.

6.14 REGISTRO DE EVENTOS (*LOGGING*)

268. 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 FortiGate, junto con las

acciones que el dispositivo ha realizado durante su escaneado en función de las políticas y perfiles de seguridad definidos.

269. 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. Por ejemplo:

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

b) Existen los siguientes ficheros de log:

c) ***Tráfico***. Registra el tráfico que atraviesa el cortafuegos 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.

d) ***Eventos***. Registra todas las acciones realizadas en la gestión y administración del dispositivo, así como la actividad del sistema FortiGate. Por ejemplo: modificaciones de la configuración, login de sesiones administrativas, eventos de Alta disponibilidad, etc.

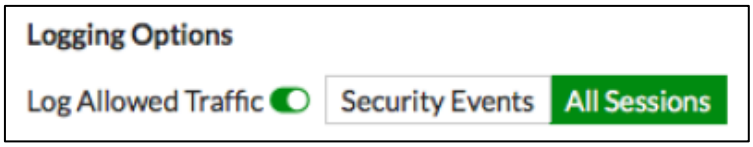
e) ***Antivirus, Web Filter, Application Control, Intrusion, Email Filter, Data Leak Prevention***. Registran las coincidencias (*match*) con las reglas configuradas en los correspondientes perfiles de seguridad. Para ello, los filtros y reglas de estos perfiles de seguridad deben tener el log habilitado, y deben estar asociados a las correspondientes políticas.

270. Cada política de seguridad debe tener habilitado el *logging* si se quiere tener registro del tráfico permitido y 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.



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.

271. **Se recomienda habilitar el log en las políticas, 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, para que quede registro de las coincidencias (*match*) encontradas por los filtros.

272. Es importante habilitar, también, el registro de todo el tráfico denegado por la política implícita por defecto del cortafuegos (*config log settings > set fwpolicy-implicit-log enable*).

273. Indicar que, en el modo de configuración seguro, el *logging* está habilitado por defecto para:

a) Nuevas políticas de seguridad.

b) Interfaces donde el acceso administrativo está habilitado.

c) Intentos de conseguir acceso administrativo en interfaces donde el acceso administrativo no esté habilitado.

d) Intentos fallidos de conexión a puertos TCP/IP distintos del 22 (ssh), 23 (telnet), 80 (HTTP), y 443 (HTTPS).

e) Todos los cambios en la configuración.

f) Fallos en la configuración.

g) Conexiones bloqueadas por alcanzar el número máximo de intentos fallidos de autenticación.

h) 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*).

274. Respecto al almacenamiento de los registros, FortiGate 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, para las unidades que no disponen de disco duro. La opción configurada cuando la memoria del sistema se llena, es la sobreescritura de los mensajes más antiguos. Todos los registros almacenados en memoria se borran cuando la unidad FortiGate se reinicia.

b) **Almacenamiento remoto**, enviando los registros a un servidor externo de auditoría a través de un canal seguro. FortiGate soporta el uso de: FortiAnalyzer, FortiCloud, y Syslog.

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

6.14.1 FORTIANALYZER

276. FortiGate 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. Es posible enviar *logs* simultáneamente a un máximo de 3 unidades FortiAnalyzer, permitiendo así una solución de *backup* para los registros.

277. Para conectarse a un dispositivo FortiAnalyzer funcionando en modo de operación seguro, es necesario instalar el certificado X.509 FortiAnalyzer en el equipo FortiGate. 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
```

278. 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*”.

279. Para más información sobre esta configuración, consultar *FortiOS Handbook* capítulo “*Logging and Reporting*”.

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

Exec ping <FortiAnalyzer IP address>

281. 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.

282. Se recomienda evitar la utilización de la característica *Test Connectivity feature* proporcionada por los equipos FortiGate.

6.14.2 SYSLOG

283. Las unidades FortiGate 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*, FotiGate solo soporta el RAW. La característica *reliable syslog* está deshabilitada por defecto, y solo puede habilitarse a través de CLI, lo cual hace que FortiGate modifique el puerto syslog por defecto (514) al puerto TCP 601.

284. 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

285. Para más información sobre esta configuración, consultar *FortiOS Handbook* capítulo "*Logging and Reporting*".

6.15 WIFI

286. La unidad FortiGate puede actuar como controlador de la red inalámbrica, gestionando las características de puntos de acceso inalámbricos (APs) de las unidades FortiAP y FortiWifi.

287. La configuración y gestión de esta función de FortiGate, se realizará desde el interfaz gráfico, en el menú ***WiFi & Switch Controller***.

288. Las unidades FortiAP son los puntos de acceso que se pueden conectar a la unidad FortiGate directamente a un puerto, o a través de un *switch* operando en L2 o L3.

289. Las unidades FortiWifi son unidades FortiGate con un punto de acceso y/o cliente inalámbrico integrado (*built-in*). Pueden funcionar en tres modos de operación:

a) Modo Punto de Acceso (modo por defecto), proporcionando un punto de acceso para clientes inalámbricos.

b) Modo Cliente, conectando la unidad FortiWifi a otras redes inalámbricas. Una unidad FortiWifi operando es este modo solo puede tener un interfaz inalámbrica.

c) Modo Monitorización, monitorizando los puntos de acceso dentro de su radio.

290. En este apartado se indican los pasos generales para configurar una red WiFi y sus puntos de acceso, así como las características relevantes de seguridad a tener en cuenta en la configuración. Para más información consultar el capítulo "*FortiWiFi and FortiAP Configuration Guide*" de *FortiOS Handbook*.

6.15.1 CARACTERÍSTICAS DE SEGURIDAD

291. En este apartado se indican varios conceptos y características de seguridad a tener en cuenta en la configuración de la red WiFi.

292. **Broadcast del SSID**. El intento de esconder la presencia de una red inalámbrica evitando el *broadcast* del SSID no mejora la seguridad de la red. Actualmente existen muchos *sniffer* que pueden detectar la red inalámbrica igualmente. Además, hay drivers que no soportan la ocultación de SSID para WPA2. Por lo tanto, no se recomienda deshabilitar el *broadcast* del SSID, ya que no mejora la seguridad y dificulta la conexión de los usuarios y aplicaciones a la red inalámbrica.

293. **Autenticación.** Hay varios tipos de autenticación disponibles para los usuarios inalámbricos:

a) Cuentas de usuarios almacenadas localmente en la unidad FortiGate.

b) Cuentas de usuario gestionadas y verificadas por un servidor externo de autenticación (RADIUS, LDAP o TACACAS+).

c) Autenticación por Directorio Activo de Windows.

Todas ellas tienen en común el uso de grupos de usuarios para especificar quién está autorizado. Para cada WLAN se creará un grupo de usuarios y se añadirán a él los usuarios autorizados para el acceso a esa WLAN. En las políticas del firewall basadas en identidad (*identity-based firewall policies*) que se creen para la WLAN, se especificarán estos grupos de usuarios permitidos.

Se recomienda el uso de un servidor externo de autenticación. Algunos puntos de acceso permiten el filtrado de MAC Address, lo cual puede ser un factor más de seguridad, pero nunca debe ser la única forma de autenticación, ya que un atacante podría capturar la MAC Address del tráfico inalámbrico y suplantar al usuario legítimo.

294. **Modo de Seguridad WPA2 - Enterprise**. El modo que, en la actualidad, proporciona la mayor seguridad en una red inalámbrica es *WPA2 Enterprise*. WPA2 tiene dos modos de implementación: *Personal*, destinado al uso en redes personales caseras

y *Enterprise*, destinado al uso en organizaciones. Ambas implementaciones difieren, principalmente, en los mecanismos de autenticación y distribución de claves. *Personal* utiliza el mecanismo de claves pre-compartidas PSK (*Pre-shared Keys*). *Enterprise* utiliza el mecanismo de autenticación 802.1X, con el empleo de un Servidor de Autenticación.

295. **Separar el acceso de empleados e invitados**. Se recomienda separar en dos redes inalámbricas distintas el acceso de invitados o proveedores, y el acceso de empleados. Esto no requiere hardware adicional, ya que los FortiAP permiten múltiples WLANs virtuales sobre el mismo punto de acceso físico. Cada una de las dos redes tendrá su propio SSID y sus propias características de seguridad, políticas de cortafuegos y autenticación de usuarios.

296. **Portal cautivo (*Captive Portal*)**. Como parte del proceso de autenticación de usuarios, se recomienda mostrar una página web en la que se indique la política de uso aceptable. Esto es un portal cautivo. Independientemente de la URL que solicite el usuario, este portal será mostrado en primer lugar. Solo después de la autenticación y aceptación de los términos y condiciones de uso, el usuario podrá acceder a los recursos solicitados.

297. **Potencia de emisión**. La cobertura de zonas no deseadas es un riesgo de seguridad potencial. Puede haber posibles atacantes en estas zonas buscando la red inalámbrica e intentando acceder. Especialmente si la cobertura de la WLAN abarca zonas públicas. Por ello, debe ajustarse la potencia de emisión a la mínima necesaria de forma que no se dé cobertura a estas zonas no deseadas.

298. **Monitorización de *rogue APs*.** Es probable que existan APs accesibles en la localización, que no forman parte de la WLAN, sino de WLANs adyacentes de otras organizaciones. Estas redes pueden causar interferencias, pero no suponen un riesgo de seguridad. El riesgo consiste en que los usuarios conecten equipos con capacidades inalámbricas y sin medidas de seguridad aplicadas, a la red cableada. Un atacante podría acceder a esos equipos a través de sus interfaces inalámbricos y obtener acceso a la red cableada. FortiGate dispone de un método para monitorizar la existencia de posibles *rogue APs*, mostrándolos en el menú del *rogue AP Monitor*, y permitiendo que un administrador pueda tomar la decisión de si se trata o no de un *rogue AP* real y suprimirlo de la red inalámbrica.

299. ***Wireless IDS* (WIDS).** El *Wireless Intrusion Detection System* (WIDS) de FortiGate, monitoriza el tráfico inalámbrico para una gama de posibles amenazas de seguridad, detectando y reportando posibles intentos de intrusión. Cuando se detecta un ataque, la unidad FortiGate registra un evento de seguridad. Se recomienda el uso de estos perfiles WIDS para detectar varios tipos de intrusiones como: *ASLEAP Attack* (Ataques contra la autenticación LEAP), *Authentication Frame*

Flooding (Ataque DoS que utiliza inundación con tramas de autenticación), etc. Los perfiles WIDS se crean desde el *WiFi & Switch Controller > WIDS Profiles*.

300. ***WiFi data channel encryption.*** Opcionalmente, se puede aplicar un cifrado DTLS a las comunicaciones entre el controlador inalámbrico y las unidades FortiAP. En las unidades FortiAP están habilitadas, por defecto, las opciones *Clear Text* y *DTLS Encryption*, por lo que es la unidad FortiGate la que determina cuál de ellas se va a utilizar según lo que se configure (a través de CLI):

```
config wireless-controller wtp-profile
edit profile1
        set dtls-policy dtls-enabled
        set dtls-policy clear-text
end
```

Si las dos opciones (DTLS y Clear Text) están habilitadas en ambos extremos (FortiAP y FortiGate), no se utilizará cifrado.

Se recomienda el uso de este cifrado, pero hay que tener en cuenta que este cifrado es basado en software y puede afectar al rendimiento. Se debe verificar si el sistema satisface los requisitos de rendimiento con este cifrado habilitado.

301. **Protected Management Frames and Opportunisitc Key Caching support.** Protected Management Frames (PMF) es una característica que protege algunos tipos de tramas de gestión como las de deauthorization, disassociation y action frames. Esta característica es obligatoria en los dispositivos certificados WiFi 802.1ac, y previene de que los atacantes envíen paquetes deauthorization/disassociation para interrumpir las conexiones o asociaciones. PMF es una especificación de la WiFi Alliance basada en IEEE 802.11w.

302. Por otro lado, existe una técnica descrita en el estándar 802.11i mediante la cual los clientes que ya han pasado por el proceso de autenticación 802.1X, pueden omitir el intercambio EAP cuando se mueven de un AP a otro (*roaming*). Esta técnica se conoce como *Pairwise Master Key caching*. Cuando un cliente se asocia por primera vez con un AP bajo la arquitectura de autenticación 802.1X, se produce un intercambio EAP seguido de un *handshake* en 4 etapas para verificar las claves de cifrado. Utilizando *PMK caching*, un AP puede "*cachear*" el identificador PMK del intercambio EAP y así, en autenticaciones posteriores, este proceso de intercambio EAP ya no se producirá, reduciendo el tiempo de autenticación.

303. Una extensión de esta técnica es OKC (*Opportunistic Key Caching*), que permite optimizar el *roaming* en capa 2 para los clientes que se mueven entre APs dentro de la misma red. Con OKC, todos los APs en la misma red de capa 2 recibirán una copia del identificador PMK de los clientes, permitiendo que los clientes autenticados 802.1X, puedan moverse de un AP a otro sin repetir la autenticación

EAP y pasando directamente al *handshake* de 4 etapas de verificación de las claves de cifrado.

El uso de PMF y OKC en una red inalámbrica es configurable solamente desde CLI:

```
config wireless-controller vap
        edit <vap_name>
                set pmf {disable | enable | optional}
                set okc {disable | enable}
        next
end
```

Cuando pmf está "*optional*" se considera habilitado, pero permitirá clientes que no utilicen PMF. Cuando PMF está "*enable*", se requerirá PMF en todos los clientes.

6.15.2 CONFIGURACIÓN DE LA RED INALÁMBRICA

304. En primer lugar, el controlador WiFi de FortiGate y su módulo de configuración en GUI se habilitarán desde CLI, si no se encuentran ya habilitados por defecto:

```
config system global
        set wireless-controller enable
end
config system settings
        set gui-wireless-controller enable
end
```

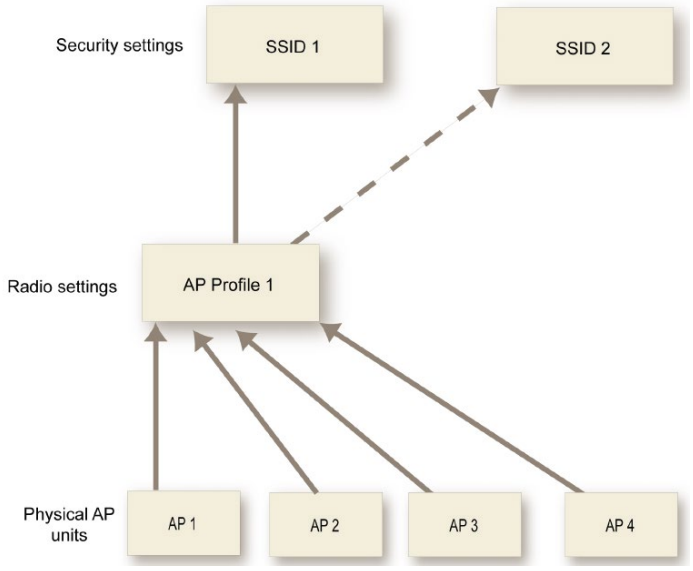
305. La configuración del controlador WiFi de FortiGate está compuesta de tres tipos de objetos: SSID, AP Profiles y los puntos de acceso físicos (APs).

a) **SSID** define el interfaz virtual de la red inalámbrica, incluyendo los parámetros de seguridad. Con un SSID es suficiente para una red inalámbrica independientemente del número de APs. No obstante, se pueden requerir varios SSIDs para proporcionar diferentes servicios o privilegios a diferentes grupos de usuarios.

b) El ***AP Profile*** (perfil AP) define los parámetros de radio, como la banda y la selección de canal. FortiGate dispone de varios AP Profiles definidos por defecto para diversos modelos de FortiAP, pero se pueden definir AP Profiles nuevos. En el AP Profile se indica también el SSID al que aplica.

c) **APs gestionados**, serán los APs que se conecten a la unidad FortiGate y sean descubiertos por esta. Cada dispositivo AP debe ser dado de alta y configurado como AP gestionado, y debe ser asignado a un AP Profile.

A continuación se muestra una visión conceptual del controlador WiFi de FortiGate:



306.El proceso para crear la red inalámbrica será el siguiente.

a) Configurar la localización geográfica.

La potencia máxima de transmisión y los canales de radio permitidos para las redes WiFi dependen de la zona geográfica donde esté la red. Por defecto, el controlador se configura para Estados Unidos.

Antes de modificar el código de país, se deben borrar todos los AP Profiles, si existen, desde WiFi & Switch Controller > FortiAP Profiles.

Para configurar el país, primero se busca el código correspondiente, y después se configura:

```
config wireless-controller setting
        set country ?
end
Con el código seleccionado (XX):
config wireless-controller setting
        set country XX
end
```

b) Crear el AP Profile.

Existen AP Profiles por defecto para varios modelos de FortiAP. En caso de que sea necesario crear un AP Profile nuevo:

- Desde WiFi & Switch Controller > FortiAP Profiles, seleccionar Create New.
- Introducir un Name para el nuevo FortiAP Profile.
- En Platform, seleccionar el modelo de FortiAP al que aplicará este profile.
- Configurar los parámetros (potencia, banda, canales, etc.).

c) Configurar el SSID.

El SSID es la interfaz de red virtual a la que se conectarán los usuarios. Para crear un SSID:

- Desde WiFi & Switch Controller > SSID, seleccionar Create New > SSID.
- Configurar los parámetros solicitados teniendo en cuenta las recomendaciones de seguridad indicadas en el apartado *6.15.1 Características de Seguridad*, en especial, el ***Security Mode*** debe ser ***WPA2-Enterprise***.

6.15.3 CONFIGURACIÓN DE LOS PUNTOS DE ACCESO

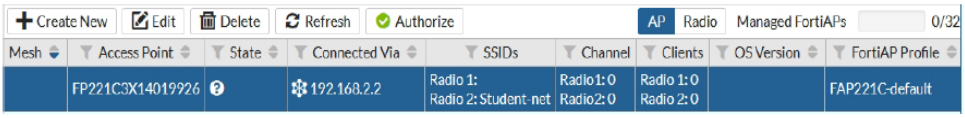
307. El primer paso para configurar un punto de acceso, es configurar el interfaz de la unidad FortiGate al que se va a conectar. Para ello los pasos serán los siguientes:

a) En la unidad FortiGate, ir a Network > Interfaces.

b) Editar el interfaz:

- *Role* debe ser LAN.
- En *Addressing Mode*, seleccionar Manual.
- En *IP/Network Mask* asignar la dirección IP y máscara de red.
- En *Administrative Access*, para IPv4 seleccionar CAPWAP (*Control And Provisioning of Wireless Access Points*).

308. Una vez configurado el interfaz, se puede conectar el AP. Transcurridos unos minutos el AP será descubierto por la unidad FortiGate y deberá reflejarse en el listado de APs en *WiFi Controller > Managed FortiAPs*.



309. Para configurar el AP, se selecciona de la lista anterior y se Edita.

   a) Opcionalmente se puede introducir un nombre (*Name*). En caso contrario, el AP será identificado por su número de serie.

   b) Asignarle el AP Profile que define los parámetros de radio para el AP y el SSID al que se conectará.

   c) Una vez configurado el AP, *Autorizarlo*.

310. Por defecto, la unidad FortiGate añade todos los APs que descubra a la lista de APs gestionados, a la espera de que sean autorizados. Para evitar que se añadan a la lista APs desconocidos, se puede deshabilitar esta función automática. En este caso solo se añadirán a la lista los APs cuyo número de serie haya sido previamente indicado de forma manual.

   Para deshabilitar esta función, se debe realizar en cada interfaz desde CLI:

```
config system interface
        edit portXX
        set ap-discover disable
end
```

311. También se pueden autorizar automáticamente los APs descubiertos sin necesidad de intervención manual, pero no esta no es una opción recomendada.

312. Se puede chequear y actualizar el firmware del FortiAP desde la unidad FortiGate que actúa como controlador WiFi.

   a) Desde la lista de los APs (WiFi & Switch Controller > Managed FortiAPs), la columna de *OS Version* indica la versión actual de firmware de cada AP.

   b) Para actualizar el firmware, seleccionar el AP, botón derecho > Upgrade Firmware.

   c) Seleccionar *Upgrade from File*. Seleccionar *Browse* y localizar el fichero de actualización del firmware.

   d) Cuando el proceso de actualización se completa, seleccionar OK. La unidad FortiAP se reiniciará.

6.15.4 MONITORIZACIÓN DE LA RED INALÁMBRICA

313. **Monitorización de los clientes inalámrbicos**. Para ver los clientes inalámbricos conectados a una unidad FortiWiFi, ir a *Monitor > Client Monitor*. Se mostrará la siguiente información:

   a) *SSID* al que el cliente está conectado.

b) *FortiAP* al que el cliente está conectado (muestra el número de serie).

c) *User* (nombre del usuario).

d) *IP* (dirección IP asignada al cliente inalámbrico).

e) *Device.*

f) *Auth* (tipo de autenticación empleada).

g) *Channel*, canal de radio WiFi en uso.

h) *Bandwidth Tx/Rx*, anchos de banda de transmisión y recepción del cliente (Kbps).

i) *Signal Strength / Noise*, el radio *signal-to-noise* en decibelios calculado a partir de la fortaleza de la señal y el nivel de ruido.

j) *Signal Strength.*

k) *Association Time*, cuánto tiempo lleva el cliente contectado al AP.

314. **Monitorización del estado de salud de la red inalámbrica.** Desde la opción *Monitor > WiFi Health Monitor*, se abre el panel "*wireless health dashboard*" que proporciona un cuadro de mando con parámetros que permiten evaluar el estado de la infraestructura de la red inalámbrica, como el estado de los APs (Active, Down, Missing), el número de clientes conectados durante un periodo de tiempo, el máximo número de clientes conectados a un AP, la información de logins fallidos, etc.

6.15.5 MONITORIZACIÓN DE *ROGUE* APS

315. El equipamiento de radio del AP puede escanear la existencia de otros APs. El AP puede hacer esta función cuando está operando en modo monitor dedicado, o cuando está operando en modo AP, conmutando cada cierto tiempo del modo operación al modo monitorización.

316. No cualquier AP detectado en el área de cobertura ha de ser un rogue AP, ya que puede tratarse de un AP perteneciente a la red inalámbrica de otra organización adyacente. Los APs que suponen una amenaza y que deben ser considerados rogue AP, son aquellos no autorizados y conectados a la red cableada. A la detección de estos APs se le llama detección de rogue AP "*on-wire*" y, en la lista del *rogue AP Monitor*, estos APs se mostrarán con una flecha verde en la columna *On-wire*.

317. Para realizar esta detección se utilizan dos técnicas simultáneamente:

a) *Coincidencia exacta de las MAC Address (Exact MAC Address match)*. Si se detecta la misma MAC Address tanto en la red inalámbrica como en la red cableada, significa que el cliente inalámbrico está accediendo a la red

cableada. En caso de que el AP a través del que accede no se encuentre en la lista de APs autorizados de la unidad FortiGate, se entenderá como un rogue AP "on-wire". Este esquema funciona para los rogue APs sin NAT.

b) *Proximidad de MAC Address (MAC Adjacency)*. Si un AP es también un router aplicará NAT a los paquetes WiFi, haciendo más difícil su detección. En este caso, la técnica que se utiliza es considerar que la MAC Address del interfaz WiFi del AP, se encontrará normalmente en el mismo rango que la MAC Address de su interfaz ethernet cableado. El escaneo buscará, por lo tanto, MAC Address en la red LAN y en la red WiFi que se encuentren dentro de una distancia máxima la una de la otra. Por defecto esta distancia es 7. Si el AP correspondiente a estas MAC Address no está autorizado, se considera como rogue AP "on-wire".

318. Esta detección de *rogue APs "on-wire"* tiene limitaciones porque requiere que, al menos, exista un cliente inalámbrico conectado al AP sospechoso y enviando tráfico constantemente. Y, si el AP es un *router*, sus MAC *Address WiFi* y LAN deben ser similares.

319. Cuando se detecta un *rogue* AP, se genera un registro de log con nivel *Alert*. Cuando se detecta un AP desconocido, se genera un registro de log con nivel *Warning.*

320. Si la función de monitorización de los APs se utiliza cuando estos operan en modo AP, implica que cada determinado tiempo (300 segundos por defecto), el AP cambiará del modo operación, al modo monitorización. Cuando el tráfico del AP sea elevado, este cambio puede causar la pérdida de paquetes de tráfico. Se puede utilizar el parámetro *ap-bgscan-idle* en CLI, para hacer que el AP solo cambie al modo monitor cuando haya estado libre de operación durante un tiempo configurable. Pero en este caso, un tráfico elevado en el AP podría causar el retraso de la monitorización.

321. Todos los APs que utilicen el mismo *AP Profile*, compartirán los mismos parámetros de escaneo de rogue APs. Para configurar la monitorización de rogue APs con la detección on-wire, desde GUI:

a) Ir a *WiFi & Switch Controller > WIDS Profiles*.

b) Seleccionar un *WIDS Profile* y editarlo, o seleccionar *Create New*.

c) Asegurarse de que *Enable Rogue AP Detection* está activado.

d) Seleccionar *Enable On-Wire Rogue AP Detection*.

322. Los APs descubiertos durante el escaneo y mostrados en *Monitor > Rogue AP Monitor*, se pueden marcar como Aceptados o como *rogue* AP de forma manual por el administrador. Para ello se selecciona el AP y en *Mark*, se selecciona *Mark Rogue*.

Solo con este marcado no se afectará a la operación de ningún cliente que esté usando estos APs. En caso de que el administrador lo considere como una amenaza real, lo puede suprimir seleccionándolo y *Suppress AP*. En este caso, el controlador WiFi de FortiGate envía mensajes "*deauthentication*", por un lado, a los clientes conectados a este AP haciéndose pasar él y, por otro lado, al AP haciéndose pasar por sus clientes.

7. FASE DE OPERACIÓN

323. Durante la fase de operación de la unidad FortiGate, 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 auditoria. 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 auditoria 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.

8. REFERENCIAS

STIC.1	CCN-STIC-807 Criptografía de empleo en el ENS
FortiOs 6.4 Administration Guide:	*https://docs.fortinet.com/product/fortigate/6.4*

9. ABREVIATURAS

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

PUBLICACIONES DE DEFENSA

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