centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1614

Procedimiento de empleo seguro
Fortinet FortiMail 6.2



Febrero 2023

MINISTERIO DE DEFENSA

cpage.mpr.gob.es

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

Edita:

MINISTERIO 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
2023.02.17 18:01:34 +01'00'

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

NIPO: 083-23-064-X.
Fecha de Edición: Febrero 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
Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

INDICE

1. INTRODUCCIÓN 5
2. OBJETO Y ALCANCE 6
3. ORGANIZACIÓN DEL DOCUMENTO 7
4. MODALIDADES DE DESPLIEGUE 8
5. FASE DE RECEPCIÓN E INSTALACIÓN 10
5.1 ENTREGA SEGURA DEL PRODUCTO 10
5.2 INSTALACIÓN SEGURA 10
5.3 REGISTRO DE LA UNIDAD 11
6. FASE DE CONFIGURACIÓN 12
6.1 ASPECTOS INICIALES 12
6.2 MODO DE OPERACIÓN SEGURO 13
6.3 ADMINISTRACIÓN DEL PRODUCTO 14
6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA 15
6.3.2 AUTENTICACIÓN DE USUARIOS 18
6.3.3 PARÁMETROS DE ADMINISTRACIÓN 22
6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 23
6.5 GESTIÓN DE CERTIFICADOS 24
6.5.1 CERTIFICADOS DE SERVIDOR 24
6.5.2 CERTIFICADOS DE CA 25
6.5.3 CRLS Y OCSP 26
6.6 PERFILES TLS 26
6.7 PERFILES DE CIFRADO IBE Y S/MIME 29
6.7.1 PERFIL DE CIFRADO IBE 29
6.7.2 PERFIL DE CIFRADO S/MIME 30
6.8 AUTENTICACIÓN DE CONEXIONES SMTP 32
6.9 SINCRONIZACIÓN 32
6.10 ACTUALIZACIONES 33
6.10.1 ACTUALIZACIÓN DE FIRMAS Y MOTORES DE INSPECCIÓN 33
6.10.2 ACTUALIZACIÓN DEL *FIRMWARE* DEL DISPOSITIVO 33
6.11 AUTO-CHEQUEOS 34
6.12 ALTA DISPONIBILIDAD 35
6.13 AUDITORÍA 37
6.13.1 REGISTRO DE EVENTOS 39
6.13.2 ALMACENAMIENTO LOCAL Y REMOTO 40
6.14 BACKUP 42
6.15 BORRADO SEGURO 44
6.16 ANTI-SPAM 44
6.16.1 DOMINIOS DE PROTECCIÓN 45
6.16.2 PERFILES 45
6.16.3 POLÍTICAS 46
7. FUNCIONALIDADES DE SEGURIDAD 47
7.1 FORTIGUARD *ANTI-SPAM* 47
7.1.1 FORTIGUARD *ANTI-SPAM DNSBL (IP BLOCK)* 48

7.1.2 FORTIGUARD *ANTI-SPAM SURBL* 48
7.1.3 BEHAVIORAL ANALYSIS....49
7.1.4 SPAM OUTBREAK PROTECTION....49
7.1.5 IMPERSONATION ANALYSIS SCAN....49
7.1.6 FORGED IP SCAN....49
7.1.7 *GREYLIST*....50
7.1.8 SPF SCAN....50
7.1.9 DMARC SCAN....50
7.1.10 *DNSBL SCAN*....51
7.1.11 SURBL SCAN....51
7.1.12 DEEP HEADER SCAN....51
7.1.13 BAYESIAN SCAN....51
7.1.14 HEURISTIC SCAN....51
7.1.15 DICTIONARY SCAN....52
7.1.16 BANNED WORD SCAN....52
7.1.17 *NEWSLETTER*....52
7.1.18 SUSPICIOUS NEWSLETTER....52
7.1.19 *SAFELIST/BLOCKLIST*....52
7.1.20 SAFELIST WORD SCAN....52
7.1.21 IMAGE SPAM SCAN....53
7.1.22 OTRAS OPCIONES....53
7.2 ACCIONES ANTI-SPAM....53
7.3 BUSINESS EMAIL COMPROMISE (BEC)....56
7.4 URI CLICK PROTECTION....56
7.5 IP BLACKLIST PROTECTION....56
7.6 RECOLECCIÓN DE DIRECTORIOS Y PREVENCIÓN DE DOS....57
7.7 CONTENT FILTERING....58
7.7.1 PERFILES DE CONTENIDO Y DICCIONARIO....58
7.7.2 ARCHIVOS COMPRIMIDOS....58
7.7.3 CONTENIDO PROTEGIDO POR CONTRASEÑA....58
7.7.4 DOCUMENTOS INCRUSTADOS....59
7.7.5 DYNAMIC DLP....60
8. FASE DE OPERACIÓN....61
9. CHECKLIST....62
10. REFERENCIAS....64
11. ABREVIATURAS....65

1. INTRODUCCIÓN

1. FortiMail es una plataforma de seguridad para correo electrónico con capacidad de pasarela (MTA) que detiene las amenazas específicas y volumétricas. Permite asegurar la superficie de ataque de la organización, evita la pérdida de datos confidenciales y ayuda a mantener el cumplimiento de la normativa.
2. FortiMail está disponible en dispositivos físicos y virtuales. Combina múltiples niveles de anti-spam y antimalware con funciones adicionales que incluyen la prevención de fuga de datos (DLP), cifrado basado en la identidad (IBE), archivado de correo electrónico y listas negras, en una solución "todo en uno".
3. Las funciones de seguridad de FortiMail, como anti-spam, antivirus, protección outbreak y protección contra amenazas avanzada están impulsadas por FortiGuard Labs. FortiMail no necesita licencias de otros proveedores y, por tanto, ofrece una solución robusta completamente integrada, sin sobrecarga adicional de licencias de terceros. Proporciona un único punto de contacto y contrato de soporte.

2. OBJETO Y ALCANCE

4. Este procedimiento aplica a todos los appliances FortiMail, ya sea en formato físico o virtual con la versión de *firmware* **6.2.** Los modelos *hardware* que han sido cualificados **en la familia de productos '*Protección de correo electrónico*"** son los siguientes:
   - *FML-200F*
   - *FML-400F*
   - *FML-900F*
   - *FML-VM (appliance virtual)*
5. Se destaca que, por ahora, el producto **no ha sido cualificado para ninguna otra familia del CPSTIC.**
6. **Las funcionalidades de Single Sing-on, DLP y FortiIsolator no han sido evaluadas y, por tanto, no se consideran cualificadas.**

3. ORGANIZACIÓN DEL DOCUMENTO

7. El documento se estructura en los siguientes apartados:

- **Apartado 4**. En este apartado se recogen las posibilidades de despliegue del producto.
- **Apartado 5.** En este apartado se recogen aspectos y recomendaciones a considerar, durante la fase de recepción e instalación del producto.
- **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.
- **Apartado 7.** En este apartado se recogen las diferentes funcionalidades de seguridad ofrecidas por el producto.
- **Apartado 8.** En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.
- **Apartado 9.** En este apartado se incluye una *checklist* con las tareas necesarias.
- **Apartado 10.** Incluye un listado de la documentación que ha sido referenciada a lo largo del documento
- **Apartado 11.** Incluye el listado de las abreviaturas empleadas a lo largo del documento.

4. MODALIDADES DE DESPLIEGUE

8. Los dispositivos FortiMail se pueden implementar en tres (3) modos:

- ***Gateway***: El modo Gateway [REF10] es el escenario de implementación más común. En este modo, FortiMail funciona como el intercambiador de correo (MTA) para el dominio e intercepta todo el correo antes de depurar las amenazas y enviarlo a su destino. La unidad FortiMail no almacena localmente ningún mensaje de correo, excepto los mensajes en cuarentena (considerados *spam*) si así se configura.

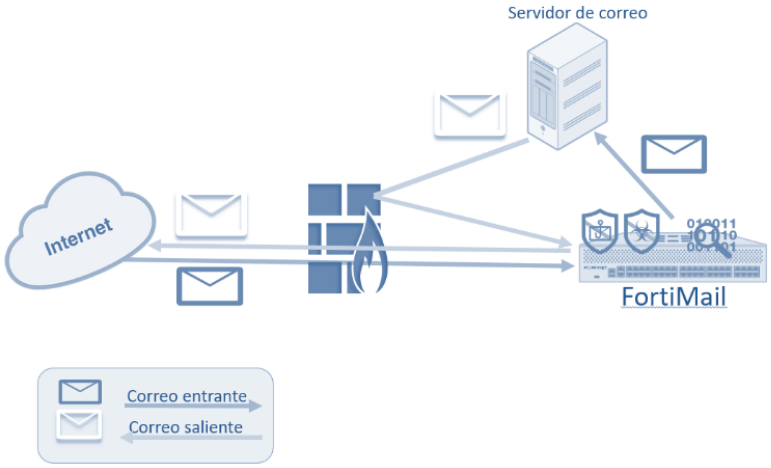


Figura 1. Modo Gateway

- ***Transparent***: En el modo transparente, la unidad FortiMail puede configurarse como *router*, y el tráfico SMTP será procesado por el dispositivo mientras que el resto del tráfico será encaminado según la tabla de rutas configurada. También, puede configurarse como *bridge*. En este caso, el tráfico que no es SMTP pasa de manera transparente por el dispositivo mientras que el tráfico SMTP es inspeccionado por el mismo. La unidad FortiMail no almacena localmente ningún mensaje de correo, excepto los mensajes en cuarentena (considerados *spam*) si así se configura.

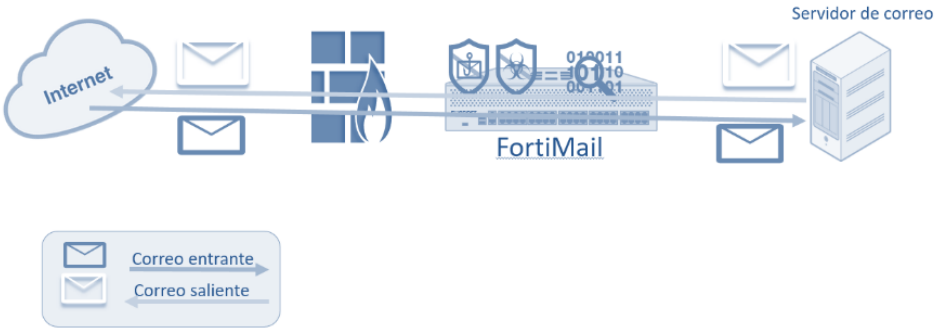


Figura 2. Modo Transparente

- ***Server***: En el modo servidor, FortiMail actúa como servidor de correo de destino proporcionando las mismas funciones de seguridad, además de proporcionar acceso al correo electrónico de los usuarios a través de POP3, IMAP4, Webmail y también sincronización de calendarios y contactos compartidos.

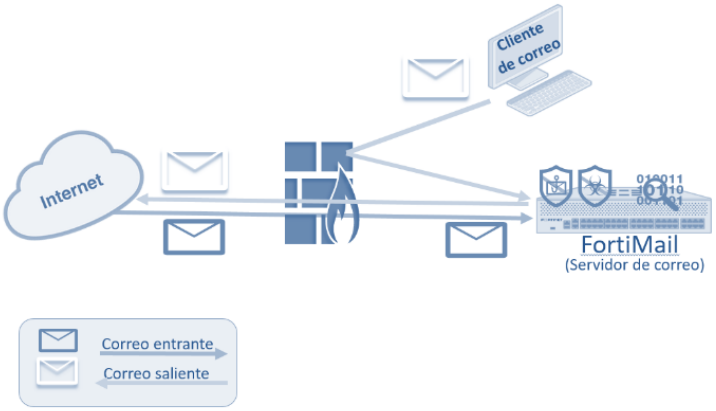


Figura 3. Modo Servidor

9. La interfaz de FortiMail webmail incluye calendario, libreta de direcciones y varias configuraciones avanzadas de usuario: como reenvío automático, respuesta automática programada o filtros de correo.

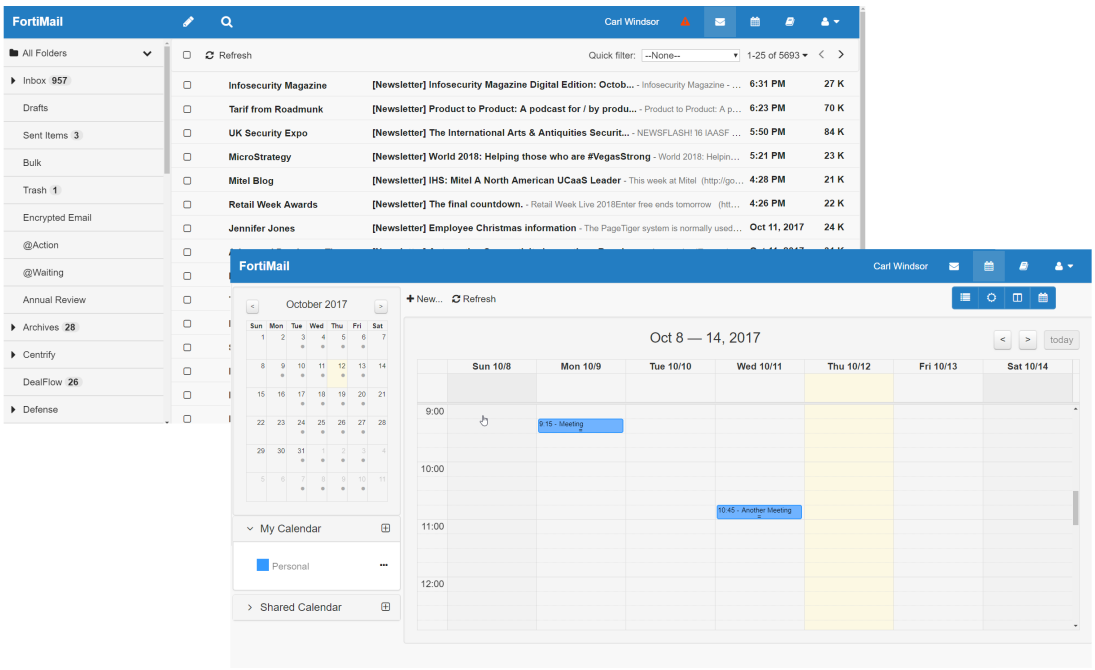


Figura 4. Vista interfaz webmail

5. FASE DE RECEPCIÓN E INSTALACIÓN

5.1 ENTREGA SEGURA DEL PRODUCTO

10. 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) **Etiqueta de envío**: Deberá comprobarse que la etiqueta de envío concuerda con la orden de compra original, y que el envío ha sido realizado directamente desde Fortinet.

    b) **Embalaje externo**: Deberá inspeccionarse el exterior de la caja de envío y la cinta adhesiva con la marca Fortinet. Se comprobará que la cinta adhesiva no esté 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 extraído el producto de la misma. El sistema de sellado deberá estar intacto.

    d) **Número de serie**: Deberá comprobarse que el número de serie del dispositivo concuerda con el enviado por el fabricante y con el que aparece en el embalaje del mismo.

    e) **Sello de garantía**: En caso de llevarlo, se deberá verificar que el sello de garantía de la unidad esté intacto. Este es una pequeña etiqueta 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.

11. En caso de identificarse algún problema durante la inspección, el usuario deberá **ponerse en contacto inmediatamente con el proveedor**, al que se le indicará el número de pedido, el número de seguimiento y una descripción del problema.

5.2 INSTALACIÓN SEGURA

12. Los dispositivos **deberán instalarse dentro de un Centro de Proceso de Datos (CPD),** cuyo acceso estará limitado a un conjunto de personas que posean una autorización expresa.

13. Para ello, la sala en la que se ubica el CPD estará dotada de un sistema de control que asegure que únicamente dichas personas pueden acceder al dispositivo (incluido fuera del horario laboral).

14. La documentación enviada junto al dispositivo incluye una guía de inicio rápida junto con un suplemento de cada *hardware* específico. La guía de administración de FortiMail proporciona información adicional sobre los procesos de instalación y

configuración. En estos documentos se encuentra información tanto del proceso de instalación del dispositivo como de su configuración inicial.

15. Para más información sobre el proceso de instalación del *firmware* en la unidad FortiMail, consultar el apartado "*Installing Firmware*" (página 578) de la Guía de Administración de FortiMail [REF1].

5.3 REGISTRO DE LA UNIDAD

16. 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* [REF13]. Esta labor se realizará siempre con la misma cuenta de usuario, de modo que sea posible gestionar la caducidad y renovaciones de mantenimiento y servicios de todos los dispositivos de forma centralizada.
17. Se deben seguir los siguientes pasos para registrar el producto:
    1. Registrarse con usuario y contraseña en la web Fortinet Support Website [REF13].
    2. En el panel lateral *Asset Management* seleccionar la opción *Register Product*.
    3. Introducir el número de serie del dispositivo y seleccionar el *End User Type* indicando si será utilizado en la administración dentro un organismo gubernamental. Continuar haciendo clic en *Next*.
    4. Completar con la información solicitada, indicando obligatoriamente en la lista desplegable *Fortinet Partner* su compañía. Continuar haciendo clic en *Next*.
    5. Leer y aceptar los términos y condiciones para terminar de registrar el dispositivo.
18. Para más detalles sobre el proceso de registro se podrá acceder a *Fortinet Support Website Guide* [REF12].

6. FASE DE CONFIGURACIÓN

6.1 ASPECTOS INICIALES

19. En el momento de la instalación de FortiMail, puede ser necesario actualizar el *firmware* a la versión cualificada 6.2. La descarga se proporciona a través de una web segura HTTPS. Primero se deberá dirigir a la página web de soporte (*https://support.fortinet.com*) [REF13] y acceder con las credencias obtenidas previamente durante el proceso de registro de la unidad.
20. Se deberá navegar hasta la página del *firmware* FortiMail 6.2, desde donde se deberá descargar. El fichero descargado tendrá que ser almacenado en el equipo de administración o en una red desde la que sea accesible desde el dispositivo FortiMail.
21. Desde el mismo directorio donde se ha obtenido el *firmware*, se deberá descargar el fichero que contendrá el MD5 del *firmware* descargado. Esta es una verificación manual, ya que al instalar el *firmware* la unidad verifica automáticamente la firma del *firmware*, mecanismo que aporta el nivel de integridad suficiente.
22. A través de una herramienta de generación de MD5 se deberá calcular el MD5 del *firmware* descargado y compararlo con el indicado en el fichero anterior. Si estos dos MD5 son iguales significará que el *firmware* que se ha descargado es el correcto y no ha habido ningún tipo de manipulación.
23. Una vez verificado el MD5, se procede a la instalación. El fichero de *firmware* viene con firma electrónica (tipo RSA-SHA512) que será verificada automáticamente por el dispositivo en la instalación (la clave pública para la verificación de la firma viene preinstalada en el dispositivo). Una vez finalizada, se verificará que la versión de *firmware* instalada es la correcta. Para ello se deberá visualizar el apartado *Dashboard > Status* en la versión GUI, o ejecutar el siguiente comando a través del CLI [REF2]:

```
get system status
```

24. Es necesario establecer el nombre del dispositivo, de modo que éste quede perfectamente identificado. Se recomienda introducir una entrada en el DNS con el nombre del equipo y la dirección IP del mismo. Para establecer el nombre de dispositivo deseado, introducir el siguiente comando a través de CLI:

```
Config system global
Set hostname <nombre_dispositivo>
```

25. Las interfaces del sistema que no vayan a ser utilizadas deben ser deshabilitadas (ver apartado 6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS), mientras las interfaces utilizadas deben ser identificadas con el uso para el que sean destinadas.

26. Para más información sobre el proceso de instalación/actualización de firmware [REF7] en la unidad FortiMail, consultar el apartado "*Installing Firmware*" (página 578) de la Guía de Administración de FortiMail [REF1].

6.2 MODO DE OPERACIÓN SEGURO

27. **Se debe configurar el modo de operación seguro, que permite al dispositivo operar según la configuración segura necesaria**. Para ello, se debe ejecutar el comando *FIPS-CC*, que solo puede habilitarse vía CLI. En caso de que el dispositivo esté ofreciendo servicio se recomienda realizar un *backup* completo antes de pasar a este modo de operación. La vuelta al modo por defecto solo se puede realizar mediante un reinicio de fábrica completo del dispositivo.

28. Para habilitar este modo de operación, se empleará el siguiente comando mediante la interfaz CLI:

```
config system fips-cc
        set status enable
end
```

29. En este momento, al operador se le solicitará una contraseña para la cuenta de administrador y se le asignará el rol de "*Crypto Officer*". Esta contraseña deberá tener una longitud mínima de 8 caracteres, pero **se recomienda un mínimo de 12** (ver apartado 6.3.3.1 POLÍTICA DE CONTRASEÑAS). Tras este proceso, el equipo se reiniciará para operar en modo de operación seguro.

30. Se deberá **comprobar que el proceso se ha completado correctamente** mediante el comando:

```
get sys status
```

31. Se mostrará la siguiente línea, que indica que el modo de operación seguro se encuentra habilitado:

```
FIPS-CC mode: enable
```

32. Se deben completar una serie de configuraciones para terminar de establecer el modo de operación seguro, las cuales se indicarán en los siguientes apartados del documento:

    a) Deben deshabilitarse los protocolos no considerados para una operación segura del producto: SSH, Telnet y HTTP.

    b) Debe configurarse el máximo número de errores de autenticación y el periodo de cuarentena hasta el próximo intento.

    c) Debe configurarse la política de las contraseñas.

    d) Debe configurarse un tiempo de inactividad de sesión.

e) Debe configurarse un mensaje de advertencia cada vez que un administrador establezca una sesión con el dispositivo (*login banner*).

6.3 ADMINISTRACIÓN DEL PRODUCTO

33. La administración y gestión del equipo **deberá atender a los principios de mínima funcionalidad y mínimo privilegio**, es decir, se procurará que los usuarios con rol de administración sean los mínimos posibles, y que el conjunto de los usuarios no disponga de más privilegios que los estrictamente necesarios para llevar a cabo sus funciones.

34. Existe una cuenta "admin" por defecto que no puede ser eliminada y cuyos atributos, nombre y permisos no pueden ser modificados. Esta cuenta cumple el rol de "*root*" (super administrador) y tiene permisos sobre todas las configuraciones de FortiMail, incluidas otras cuentas de administrador y sus contraseñas. Se puede consultar información detalladas sobre esta cuenta en el apartado *"About the admin account*" (página 182) de la Guía de Administración de FortiMail [REF1].

35. Previamente a crear una cuenta de administración, se debe crear un *Admin Profile* al que se asignará la cuenta. El *Admin Profile* junto con el dominio asignado a la cuenta, determinarán qué comandos puede ejecutar y a qué áreas podrá acceder el administrador.

36. El dominio puede ser:

    - ***System*:** permite acceder a cualquier área, independientemente de si esta pertenece a la unidad FortiMail o a un dominio protegido.
    - ***Dominio protegido*:** permite acceder únicamente a las áreas que estén asignadas a ese dominio protegido. No permite acceder a configuraciones de sistema de la unidad FortiMail, ni a CLI.

37. Los *Admin Profiles* establecen permisos de lectura (para ver configuraciones), escritura (para modificar configuraciones) o no acceso, a cada una de las áreas. Estas son: listas blancas/negras, cuarentena, Políticas, Archivado de correos, etc.

38. El Admin Profile se crea desde *System > Administrator > Admin Profile*. Hacer clic en *New*, introducir el nombre deseado para el perfil y en la tabla *Access Control*, seleccionar los permisos deseados.

39. Para configurar o modificar cuentas de administración se han de seguir los siguientes pasos:

    1. Acceder a *System > Administrator > Administrator*
    2. Seleccionar una cuenta de administrador para modificarla o hacer click en *New* para crear una nueva.
    3. Configurar los campos necesarios y finalmente seleccionar *Create.*

40. Entre los campos a rellenar se encontrarán el Admin Profile, Domain y, también:

- ***Authentication Type***: tipo de autenticación, que puede ser PKI (certificado cliente), local (contraseñas), RADIUS o LDAP. En el apartado 6.3.2 AUTENTICACIÓN DE USUARIOS se detallan estos tipos de autenticación.
- ***Trusted Hosts*****:** para indicar la lista de IPs o subredes desde los que el administrador podrá conectarse únicamente.

41. Para más información acerca de la configuración de administradores, consultar el Apartado "*Configuring administrator accounts and Access profiles*" (página 179) de la Guía de Administración de FortiMail [REF1].

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

42. La administración del dispositivo podrá realizarse de manera local o remota.
    - Administración local**:** puede realizarse desde un terminal empleando la interfaz de línea de comandos (CLI). Para ello, será necesario conectar un equipo de administración mediante cable ethernet al interfaz de red correspondiente de la unidad FortiMail.
    - Administración remota**:** el dispositivo permite emplear el protocolo HTTPS para llevar a cabo la gestión remota a través de la web GUI.
43. Asimismo, también está disponible el acceso vía API basada en REST para monitorización, automatización y orquestación. Para garantizar este acceso se deberá asignar el rol de API a los administradores que lo requieran.

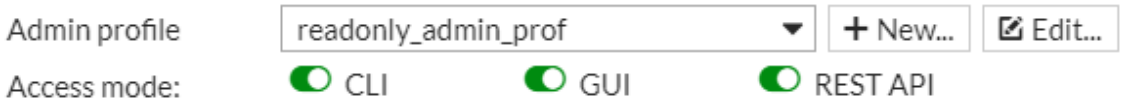


Figura 5. Acceso via API.

44. Para habilitar el acceso mediante el protocolo HTTPS a la interfaz gráfica (GUI), se debe usar una conexión de consola local y realizar los siguientes pasos:
    1. Empleando un cable de red, conectar directamente el puerto de red de la unidad FortiMail al puerto de red del equipo del administrador.
    2. Anotar el número/identificador del puerto de red físico.
    3. Usando una conexión de consola local, conectarse al CLI.
    4. Introducir los siguientes comandos:
        a) *Config system interface*
        b) *Edit <interface_name>*
        c) *Set allowaccess https*
        d) *End*

5. Para confirmar la configuración:

   a) *Show system interface <interface_name>*

45. **Debe habilitarse para la administración remota únicamente HTTPS. Los protocolos Telnet, HTTP y SSH deben estar deshabilitados**. Esto se verificará por cada uno de los interfaces que se hayan habilitado, desde *System > Network > Interface*, haciendo clic sobre la interfaz deseada:

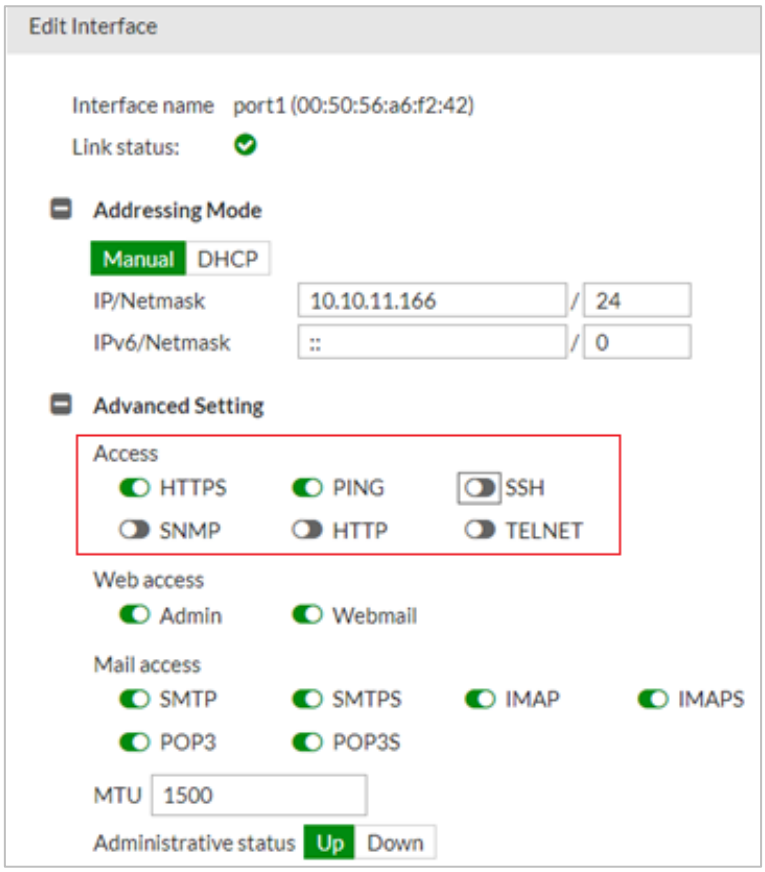


Figura 6. Configuración de interfaces y acceso remoto.

46. Para que la unidad FortiMail opere en modo seguro:

   a) La versión TLS que utilizará es **TLSv1.2**. En caso de que fuese necesario configurarlo de forma manual, se debería utilizar el siguiente comando:

```
config sys global
    set ssl-versions tls1_2
end
```

   b) Las cipher suites que utilizará para TLS Server son las siguientes:

   - *TLS_DHE_RSA_WITH_AES_128_CBC_SHA*
   - *TLS_DHE_RSA_WITH_AES_256_CBC_SHA*
   - *TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256*

- *TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256*
- *TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256*
- *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384*

c) Utilizará Grupos Diffie Hellman con parámetros de **4096 bits**. En caso de que fuese necesario habilitarlos de forma manual, se debería utilizar el siguiente comando:

```
config sys global
    set dh-params 4096
end
```

d) La unidad FortiMail dispone por defecto de un certificado autofirmado. En la primera conexión al GUI este certificado debe aceptarse por el administrador para poder realizar el login. Se recomienda que, posteriormente este certificado sea sustituido por un certificado firmado por una CA de confianza, y que sea un **certificado tipo RSA con clave igual o superior a 3072 bits**. Para ello, seguir los pasos indicados en el apartado 6.5 GESTIÓN DE CERTIFICADOS sobre la Gestión de Certificados.

47. Una vez habilitada la administración remota GUI, para conectarse a ella se seguirán los siguientes pasos:

1. Configurar el equipo de gestión en la misma subred en la que se encuentra configurada la interfaz de red de la unidad FortiMail (192.168.1.0/24 por defecto).
2. Usando un cable Ethernet, conectar el equipo de gestión al puerto de la unidad FortiMail.
3. Lanzar un navegador web e introducir la URL https://192.168.1.99/admin
4. Como se ha indicado anteriormente, verificar y aceptar de forma temporal el certificado autofirmado del que dispone por defecto el dispositivo. No se puede llevar a cabo el proceso de login sin aceptar antes el certificado.
5. En el campo *Name*, escribir “admin”, a continuación, seleccionar *Login*.
6. El navegador web del cliente empleado para la conexión, deberá soportar TLS 1.2.

48. Como medida de seguridad adicional se recomienda limitar el acceso de cada administrador a la gestión remota, desde ciertas IPs o subredes. Para ello se

```
config system admin
  edit "admin"
    set trusthost 172.16.0.0 255.240.0.0
end
```

rellenará el campo Trusted Host de la cuenta de administrador, o se utilizarán los siguientes comandos CLI:

6.3.2 AUTENTICACIÓN DE USUARIOS

49. La autenticación tanto de usuarios de correo, como de administradores de la unidad FortiMail, puede realizarse de las siguientes formas:
    a) Autenticación Local: usuario y contraseña.
    b) Autenticación con servidores externos: LDAP o RADIUS.
    c) Autenticación PKI: con certificado cliente X.509v3.
50. Se recomienda utilizar autenticación local o PKI. Cuando se da de alta un administrador o un usuario de correo, se deberá seleccionar en el campo *Authentication Type*, el tipo de autenticación.

6.3.2.1 AUTENTICACIÓN CON CERTIFICADO

51. La autenticación con certificado (*PKI Authentication*) está disponible para los usuarios administradores y para los usuarios de webmail en caso de que se haya establecido FortiMail en modo servidor.
52. Cuando se configura la autenticación por certificado, el usuario o administrador se conecta a la unidad FortiMail y presenta el certificado cliente. Como pre-requisito, el certificado de la CA emisora de estos certificados clientes, debe estar instalado en la unidad FortiMail.
53. Si la unidad FortiMail considera válido el certificado cliente, permitirá la conexión. Si no, se comportará según haya configurado el administrador, fallando la conexión o solicitando el usuario y contraseña.
54. Para la configuración del comportamiento de FortiMail ante certificados, se podrá establecer para **usuarios de correo** la obligación de presentar un certificado válido mediante CLI:

```
config policy recipient
  edit <policy_index>
    set certificate-required yes
end
```

Donde:

- *<policy_index>:* índice que numera las políticas del sistema. Para consultar una lista de las políticas existentes se puede introducir en el CLI una interrogación *(?).*

55. Establecer *set certificate-required* ***no*** supondrá la solicitud de usuario y contraseña al usuario de correo una vez haya fallado la validación del certificado.

56. También se podrá establecer la exigencia de un certificado válido para **usuarios administradores** en la autenticación PKI mediante los comandos:

```
config system global
    set pki-certificate-req yes
end
```

57. Para que un certificado de cliente sea válido, debe cumplir una serie de condiciones, entre las que se incluyen:
    - No debe haber expirado.
    - No debe haber sido revocado.
    - Debe estar firmado por una Autoridad de Certificación (CA) de confianza, cuyo certificado haya sido importado en la unidad FortiMail.
58. Por cada usuario o administrador que utilicen esta autenticación debe crearse un *PKI User* para los tipos de usuario:
    a) Usuario administrador: al crear la cuenta de administración, se seleccionará el *Authentication Type: PKI* y se le asignará el PKI User creado.
    b) Usuario de correo: debe habilitarse la autenticación con PKI en las políticas de correo entrante (*inbound policies*) que se apliquen a esos usuarios de correo. Para ello desde *Policy > Recipient Policy,* seleccionar o crear la política deseada, en el apartado *Advanced Settings,* habilitar *Enable PKI authentication for webmail Access.*
59. El *PKI User* se crea desde *Domain & User > User > PKI User*. Entre los parámetros a rellenar, se encuentran:
    a) **Nombre del *PKI User*:** normalmente se pondrá el mismo nombre que la cuenta de usuario o administrador.
    b) ***Domain***: dominio al que el usuario estará asignado.
    c) ***CA*:** nombre del certificado de la CA a utilizar para validar la firma de la CA del certificado cliente.
    d) ***Subject*:** valor del campo subject del certificado cliente.
    e) ***LDAP query*:** se habilitará este campo si queremos consultar a un directorio LDAP, la existencia del PKI User. En este caso será necesario haber configurado un LDAP profile, que deberá seleccionarse aquí.
    f) ***OCSP*:** se habilitará si queremos utilizar un servidor OCSP para verificar si el certificado cliente ha sido revocado. En este caso, habrá que configurar otros valores, como la URL del servidor. En el apartado 6.5.3 CRLs y OCSP se incluye más información acerca de esta configuración.

60. Para habilitar la autenticación por certificado para todos los *PKI Users*, hay que ejecutar el siguiente comando a través del CLI en la unidad FortiMail:

```
config system global
    set pki-mode enable
end
```

61. Para cada *PKI user*, se debe importar el certificado cliente en el navegador de cada equipo.

62. Para más información sobre el proceso de autenticación mediante PKI, consultar el apartado "*Appendix F: PKI Authentication*" (página 636) de la Guía de Administración de FortiMail [REF1].

6.3.2.2 AUTENTICACIÓN CON SERVIDORES LDAP O RADIUS

63. El proceso de autenticación de usuarios y administradores también puede llevarse a cabo mediante servidores de autenticación externos tipo LDAP o RADIUS. Cuando FortiMail opera en modo servidor, solo es posible utilizar autenticación local o RADIUS.

64. Para ello, cuando se crean las cuentas de usuario o administrador debe seleccionarse el *Authentication Type: RADIUS o LDAP*. Esto requiere seleccionar el correspondiente perfil de autenticación RADIUS o LDAP, que habrá sido previamente creado.

65. Perfiles de Autenticación RADIUS: para configurar un perfil de autenticación RADIUS que, entre otras cosas, indicará el servidor RADIUS a emplear para la autenticación y otros parámetros necesarios, se deben seguir los siguientes pasos:

    1. Ir a *Profile* > *Authentication* > *RADIUS*
    2. Hacer click en *New* para añadir un nuevo perfil, o seleccionar un perfil existente para modificarlo.
    3. Configurar los campos necesarios y guardar la configuración.

66. Entre los campos a rellenar se encuentran:

    - *Domain*: seleccionar *system* si se quiere aplicar el perfil a todo el sistema Fortimail; seleccionar el nombre de un *protected domain* si se quiere aplicar únicamente a ese dominio.
    - *Server name/IP*: nombre o dirección IP del servidor RADIUS.
    - *Protocol*: Selecciona el protocolo de autenticación del servidor RADIUS.

67. Para más información al respecto, consultar el apartado "*Configuring authentication profiles*" (página 445), de la Guía de Administración de FortiMail [REF1].

68. Perfiles de Autenticación LDAP: para configurar un perfil de autenticación LDAP que, entre otras cosas, indicará el servidor LDAP a emplear para la autenticación y otros parámetros necesarios, se deben seguir los siguientes pasos:
    1. Ir a *Profile > LDAP > LDAP*
    2. Hacer click en *New* para añadir un nuevo perfil, o seleccionar un perfil existente para modificarlo.
    3. Configurar los campos necesarios y guardar la configuración
69. Entre los campos a rellenar se encuentran:
    - *Server name/IP*: nombre o dirección IP del servidor LDAP.
    - *Use secure connection*: elegir si se establecerá una conexión cifrada. Para una configuración segura, se debe seleccionar *SSL* para establecer una conexión LDAPS.
    - *Base DN:* establece el nombre distinguido (DN) del árbol de directorios LDAP como base de búsqueda.
    - *Bind DN*: establecer el "bind DN" de un usuario LDAP con permisos para realizar "queries" en el "base DN"
    - *Bind Password*: establece la contraseña del "bind DN"
70. Dentro de *Advanced options* se puede configurar:
    - *Protocol version*: seleccionar el protocolo LDAP utilizado por el servidor**. Se recomienda el uso de *LDAP Version 3* para una configuración segura.**
    - *Enable webmail password change*: habilita la posibilidad a los usuarios de webmail de cambiar sus contraseñas.
    - *Password schema*: establece *OpenLDAP* o *Active Directory* como esquema de usuarios y contraseñas en el servidor.
71. Para más información acerca del proceso de configuración de perfiles de autenticación LDAP, consultar el apartado "*Configuring LDAP profiles"* (página 448) de la Guía de Administración de FortiMail [REF1].

6.3.2.3 AUTENTICACIÓN CON CONTRASEÑAS

72. El proceso de autenticación de usuarios y administradores también se puede llevar a cabo con usuario / contraseña. Para ello, cuando se crean las cuentas de usuario o administrador debe seleccionarse el *Authentication Type: Local* e introducir la contraseña en el campo *Password*.
73. La contraseña deberá cumplir la política de contraseñas que haya sido configurada por los administradores (ver Apartado 6.3.3.1 POLÍTICA DE CONTRASEÑAS).

6.3.3 PARÁMETROS DE ADMINISTRACIÓN

6.3.3.1 POLÍTICA DE CONTRASEÑAS

74. La autenticación por usuario y contraseña se utilizará en aquellas cuentas de usuario o administrador con Tipo de Autenticación (*Authentication Type*): Local.

75. Los administradores pueden establecer políticas de contraseñas (*Password Policy*), especificando longitudes mínimas y caracteres admitidos. Estas políticas aplicarán a las contraseñas de los administradores, usuarios de FortiMail Webmail, y usuarios de emails cifrados IBE (ver apartado 6.7.1 PERFIL DE CIFRADO IBE).

76. A través del interfaz web, desde *System > Configuration > Option*. Los parámetros que permite configurar son:

    - *Minimum-length:* longitud mínima de contraseña. **Se recomienda un mínimo de 12 caracteres.**
    - *Must-contain:* caracteres que debe incluir la contraseña. **Se recomienda seleccionar: mayúsculas (*Uppercase letters*), minúsculas (*Lowercase letters*), números (*Numbers*) y caracteres especiales (*Non alphanumeric character*).**

77. A través de comandos CLI:

```
config system password-policy
        set status {enable|disable}
        set apply-to admin-user
        set minimum-length <integer between 8-15>
        set must-contain {lower-case-letter non-alphanumeric number upper-case
        letter}
end
```

6.3.3.2 CONFIGURACIÓN DE PARÁMETROS DE SESIÓN

78. Debe limitarse el tiempo de inactividad de sesión para la gestión del equipo, siendo **recomendable un valor no superior a los 5 minutos**. Los comandos CLI para ello, son los siguientes:

```
config system global
  set admin-idle-timeout 5
end
```

79. Debe limitarse el **número máximo de intentos fallidos de autenticación**. La unidad FortiMail soporta entre 3 y 5 intentos inválidos. **Se recomienda un máximo de 3 intentos**. Los comandos CLI para ello, son los siguientes:

```
config system global
  set admin-lockout-threshold 3
end
```

80. Debe configurarse el **tiempo de bloqueo** establecido tras superar el número máximo de intentos fallidos de autenticación. Se recomienda un tiempo mínimo de **5 minutos**. Los comandos CLI para ello, son los siguientes:

```
config system global
  set admin-lockout-duration 5
end
```

81. En caso de producirse el bloqueo de cuentas de administración, la unidad FortiMail permitiría el acceso de administración a través de la consola física, sin necesidad de configuración adicional.

82. *Login Banner*: el dispositivo ofrece la capacidad de mostrar mensajes de aviso y consentimiento, configurables por usuarios con perfil de administración. Dichos mensajes pueden ser mostrados tanto antes como después del proceso de autenticación. Los comandos CLI para ello, son los siguientes:

```
config system global
  set post-login-banner {admin|ibe|webmail}
  set pre-login-banner admin
```

83. Estos mensajes también se pueden configurar desde la interfaz web, en *System > Configuration > Option*.

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

84. **Se deben deshabilitar las interfaces que no estén en uso en el dispositivo**, con el objetivo de minimizar los riesgos de exposición a ataques.

85. A continuación, se muestra el comando a emplear para deshabilitar una interfaz:

```
config system interface
    edit <interface>
      set status down
end
```

86. Esta opción también está disponible desde la interfaz web, en la opción *System > Network > Interface.*

6.5 GESTIÓN DE CERTIFICADOS

87. El producto soporta el uso de certificados X.509v3:

- Certificados de servidor: la unidad FortiMail presentará certificados de servidor para las siguientes conexiones:
  1. Administración web UI (conexiones HTTPS).
  2. Webmail (conexiones HTTPS).
  3. Conexiones para correo seguro, como SMTPS, IMAPS y POP3S.
- Certificados de CAs: para la validar los certificados que servidores o clientes presenten a la unidad FortiMail.
- Certificados personales de los usuarios de correo, empleados para el cifrado S/MIME (ver apartado 6.7.2 PERFIL DE CIFRADO S/MIME).

6.5.1 CERTIFICADOS DE SERVIDOR

88. Desde *System > Certificate > Local Certificates* se pueden visualizar los certificados de servidor firmados que están instalados en la unidad FortiMail, y las solicitudes de firma de certificados generadas (CSRs).

89. Desde esa opción se pueden también generar nuevas peticiones de certificado CSRs, e importar e instalar certificados firmados. Para generar una petición CSR, se debe acceder a *System > Certificate > Local Certificates: Generate* y rellenar la información solicitada:

a) Nombre del certificado.

b) IDType para especificar qué tipo de identificador se usará:

- *HostIP*: requiere que la unidad FortiMail tenga asignada una IP pública estática. Esta será introducida en el campo IP.
- *Domain name*: requiere que la unidad FortiMail tenga un FQDN (*fully-qualified domain name*). Este será introducido en el campo *Domain Name.*
- *e-mail*: requiere una dirección de correo de la unidad FortiMail o de la persona responsable de la misma. Este email será introducido en el campo email.

c) Opcionalmente: Unidad organizativa, organización, localidad, estado/provincia, país.

d) *Key Type y Key Size*: como se ha indicado en el apartado 6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA relativo a la administración remota, **debe seleccionarse el tipo de clave RSA con un tamaño de 3072 bits para cumplimiento de la CCN-STIC-807.**

90. Una vez generada la petición CSR, se deberá descargar seleccionándola de *System > Certificate > Local Certificates* y pulsar *Download*. Esto genera el fichero .csr que debe ser enviado a la CA para firma.

91. La unidad FortiMail permite importar certificados en formato PEM o PKCS#12. Si el certificado a importar ha sido firmado por una CA intermediaria en lugar de una CA *root*, para que los clientes confíen en ese certificado del servidor hay dos (2) opciones:

    - Instalar cada uno de los certificados de CAs intermedias en la lista de CAs de confianza del cliente.
    - Incluir una cadena de firma en el certificado de servidor de la unidad FortiMail.

92. La segunda opción es más sencilla a nivel de despliegue. Para ello, antes de importar el certificado servidor en la unidad FortiMail, debe editarse el fichero del certificado con un editor de texto y anexar el certificado de cada CA intermedia en orden (partiendo de la CA intermedia que firmó el certificado a importar, y finalizando con la CA intermedia cuyo certificado está firmado por la CA root). Por ejemplo:

```
-----BEGIN CERTIFICATE-----
<certificado local de servidor de la unidad FortiMail>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<certificado de la CA intermedia 1, que firmó el certificado de
la unidad FortiMail>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----

<certificado de la CA intermedia 2, que firmó el certificado de
la CA intermedia 1 y cuyo certificado ha sido firmado por una CA
root de confianza>
-----END CERTIFICATE-----
```

93. El certificado local de servidor se importará desde: *System > Certificate > Local Certificates: Import*.

6.5.2 CERTIFICADOS DE CA

94. La unidad FortiMail debe tener instalados los certificados de las CAs correspondientes, para validar los certificados que le presenten tanto los usuarios como otros dispositivos.

95. Como se ha comentado en apartados anteriores, para validar un certificado que otro dispositivo le presente a la unidad FortiMail, este debe tener instalado el certificado de la CA emisora. En caso de que se haya usado más de un nivel de CA para la emisión del certificado, deberán importarse en la unidad FortiMail todos los certificados de las CAs intermedias y de la CA root. Si alguno de estos certificados no se encuentra en FortiMail, se romperá la cadena de confianza y fallará la validación del certificado presentado.

96. Para ver la lista de los certificados de CA instalados o importar nuevos certificados de CAs en la unidad FortiMail, ir a *System > Certificate > CA Certificate*.

6.5.3 CRLS Y OCSP

97. Para verificar el estado de revocación de los certificados, se pueden usar Listas de Revocación de Certificados (CRLs) o consultas OCSP (online certificate status protocol).

98. Las listas CRL se pueden visualizar, importar o borrar desde *System > Certificate > Certificate Revocation List*.

99. Respecto a OCSP, en la configuración de los PKI User (usuarios y administradores que se autenticarán a través de certificado), se indica en la sección OCSP:

    - Si la opción de verificación de revocación del certificado por OCSP, está o no habilitada.
    - La URL del servidor OCSP.
    - La acción a realizar en caso de que no haya conexión con el servidor OCSP: *Ignore* (el dispositivo permite autenticarse al usuario) o *revoke*: el dispositivo se comporta como si el certificado estuviese revocado. Se recomienda configurar esta última.

100. Si se utiliza OCSP, los certificados de los servidores OCSP que se utilicen deben haber sido importados desde *System > Certificate > Remote > Import.*

101. Para más información sobre la gestión de certificados, consultar el Apartado "*Managing certificates*" (página 275) de la Guía de Administración de FortiMail [REF1].

6.6 PERFILES TLS

102. FortiMail soporta SMTPS (SMTP sobre TLS) y STARTTLS para el envío y recepción de correo.

103. **Recepción de correo**: SMTPS corre sobre un puerto (465) distinto del puerto habitual de correo. Desde *System > Mail Settings > Mail Server Settings*, **se debe activar la opción *SMTP over SSL/TLS*.** Esto permite que la unidad FortiMail admita conexiones TLS desde clientes SMTP y MTAs. Si está deshabilitado, las conexiones con la unidad Fortinet ocurrirán en texto claro.

104. Sin embargo, que FortiMail admita conexiones SMTP sobre TLS no quiere decir se obligue a los clientes a usarlas. Para forzar el uso de TLS en las conexiones entrantes, es decir, iniciadas por un cliente SMTP, **deberán configurarse las correspondientes reglas de control de acceso para la recepción de mensajes (*Access Control Rules*) asignándoles un *Perfil TLS*.**

105. Con respecto a la entrega de correo, no hay ninguna opción global sobre cómo se comporta la unidad FortiMail en la entrega de mensajes a la MTA siguiente. Por defecto usará la opción STARTTLS, lo que significa que:

    - Si la MTA receptora admite STARTTLS, la unidad FortiMail utilizará TLS e inicia una sesión a través de la cual enviará los mensajes.

- Si la MTA receptora no admite STARTTLS, la unidad FortiMail utilizará SMTP y enviará los mensajes sin cifrar.
- Si la MTA receptora admite STARTTLS, pero la sesión TLS no puede establecerse, la unidad FortiMail hará un *fallback* a SMTP y enviará los mensajes sin cifrar.

106. Dado que este comportamiento global de la unidad FortiMail respecto a conexiones TLS puede no ser el requerido en la organización, para dar mayor flexibilidad existen los ***Perfiles o Profiles TLS***.

107. Estos se configuran en las reglas de control de acceso que aplican a los correos entrantes (*Access Control Rules*) o a los correos salientes (*Delivery Rules*).

108. En cada una de estas reglas se puede asignar un Perfil TLS que aplicará a todos los correos que hagan match con esas reglas. Mediante el Perfil TLS se puede forzar a que las conexiones entrantes para recepción de correos (iniciadas por un cliente SMTP) o las conexiones salientes para la entrega de correos (iniciadas por la unidad FortiMail), deban utilizar TLS y, además, con cierto nivel de cifrado y con validación de certificados.

109. Los perfiles TLS se configuran desde el menú *Profile > Security > TLS.*

- Hacer click en *New* para añadir un nuevo perfil, o seleccionar un perfil para modificarlo.
- Para la creación de un nuevo perfil, introducir un nombre válido en el campo *Profile name*. Este nombre podrá ser editado más tarde.

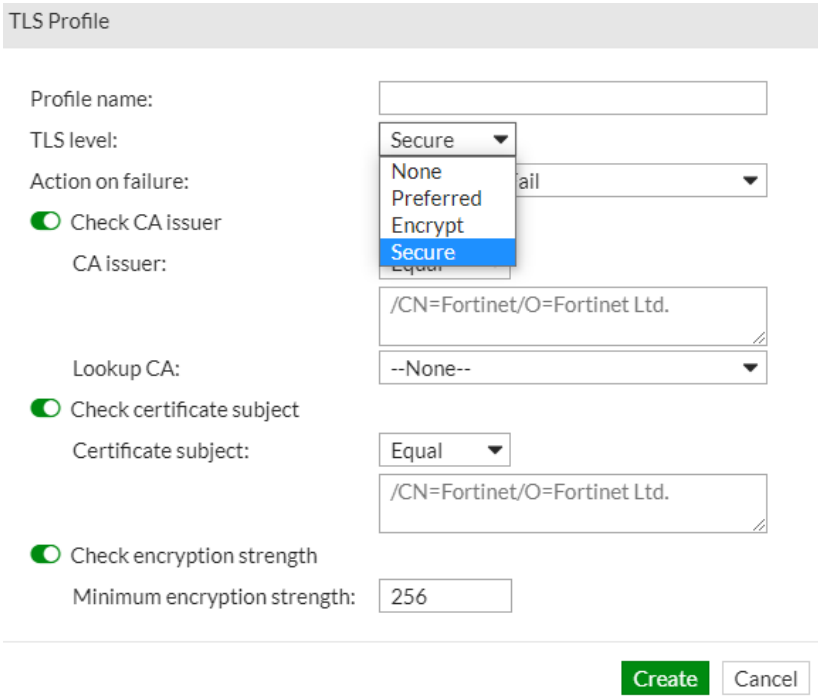


Figura 7. Perfil de seguridad TLS

110. Los parámetros a configurar serán los siguientes:

- TLS Level:

    a) *None*: deshabilita TLS. La unidad FortiMail no aceptará TLS en las conexiones entrantes (no aceptará el comando STARTTLS del cliente), o bien no iniciará TLS en las conexiones salientes (incluso si STARTTLS lo anuncia la MTA receptora).

    b) *Preferred*: el uso de TLS dependerá de la otra parte de la conexión. La unidad FortiMail aceptará conexiones entrantes TLS, pero no será obligatorio, también aceptará las que no sean TLS. Respecto a las salientes, intentará el establecimiento de TLS, pero si el destino no lo acepta, establecerá igualmente la conexión.

    c) *Encrypt*: aceptará y establecerá solo conexiones TLS. Si se produce fallo en la negociación TLS con la otra parte, ejecuta la acción del *Failure* establecida en el perfil.

    d) *Secure*: aceptará y establecerá solo **conexiones TLS con autenticación por certificado**. El fallo en la negociación TLS o en la validación del certificado de la otra parte, ejecutará la acción del Failure configurada en el Perfil. Los certificados de las CAs correspondientes deben ser instalados en la unidad FortiMail. **Se debe configurar esta opción.**

- Action on Failure:

    a) *Temporary Fail*: si la sesión TLS no puede establecerse la unidad FortiMail fallará la conexión temporalmente y lo intentará más tarde. No se envía ninguna notificación al emisor.

    b) *Fail*: si no se puede establecer la sesión TLS, la unidad FortiMail fallará inmediatamente la entrega del correo, y enviará un mensaje notificando al emisor dicho fallo.

- *Check CA issuer / campo CA issuer:* permite introducir un valor en el campo CA issuer que va a comparar con el campo *issuer* de los certificados de CA instalados en la unidad FortiMail. Solo aplica para conexiones *Secure*.
- *Check certificate subject / campo Certificate subject*: permite introducir un valor en el campo *Certificate subject* que va a comparar con el campo *Subject* de los certificados de CA instalados en la unidad FortiMail. Solo aplica para conexiones Secure.
- *Check encryption strength / campo Minimum encryption strength*: permite introducir un valor en el campo *Minimum encryption strength* que representa la longitud mínima de la clave de cifrado. Solo válido para *Encrypt* y *Secure*.

111. Como se ha indicado en apartados anteriores, cuando el dispositivo opera en el modo de operación seguro, la unidad FortiMail está configurada de forma global para utilizar **TLS 1.2**, utilizando las siguientes cipher suites:

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (solo cliente)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (solo cliente)

112. Con esta configuración, la longitud mínima de la clave de cifrado AES es 128 bits, por lo que no es necesario especificar ninguna otra en *Check encryption strength* para cumplimiento de la CCN-STIC-807. **En otras circunstancias, sería necesario especificar 128 bits en este campo del *TLS Profile*.**

113. Sí será necesario, como se ha comentado en apartados anteriores, utilizar **certificados de tipo RSA con claves de, al menos, 3072 bits** (ver apartado 6.5 GESTIÓN DE CERTIFICADOS).

114. Para más información acerca del proceso de configuración de perfiles de seguridad TLS, consultar el apartado "*Configuring security profiles*" (página 483) de la Guía de Administración de FortiMail [REF1].

6.7 PERFILES DE CIFRADO IBE Y S/MIME

115. La unidad FortiMail permite configurar *Perfiles de cifrado* que contienen los parámetros de cifrado para S/MIME y para el cifrado basado en identidad (*Identity-based Encryption,* IBE).

116. Los perfiles de cifrado pueden ser configurados en *Profile > Security > Encryption.* En el momento de la creación de un perfil, se selecciona a qué protocolo se asigna S/MIME o IBE.

6.7.1 PERFIL DE CIFRADO IBE

117. El esquema de cifrado IBE [REF5] permite aplicar un cifrado a los correos dependiendo del cliente o usuario que haga uso de la plataforma, y empleando una clave generada a partir de las direcciones de correo del remitente/ destinatario u otros parámetros.

118. Cuando un mensaje de correo llega a la unidad FortMail, y existe configurado un perfil de cifrado IBE en la correspondiente política o regla asociada, la unidad cifra el correo usando la clave asociada al receptor y le envía a este una notificación. Esta clave la habrá generado la unidad basándose en su dirección de correo. El receptor no necesita instalar ningún software ni generar claves para acceder al mensaje, ya que la notificación contiene un adjunto HTML con las instrucciones y enlaces necesarios para indicarle como acceder al correo cifrado. Cuando el receptor se

conecta a la unidad FortiMail y sigue las instrucciones, el email se descifra de forma automática.

119. **Este perfil de cifrado IBE debe estar configurado**. Para ello, se debe acceder a *Profile > Security > Encryption*, seleccionando *Protocol: IBE*. Algunos de los parámetros a rellenar serán los siguientes:

- *IBE Action*: acción utilizada por los receptores para obtener los mensajes IBE.
  a) *Push*: se entrega al receptor una notificación y el email seguro. El receptor debe ir a la unidad FortiMail para abrir el mensaje. La unidad FortiMail no almacena el mensaje.
  b) *Pull*: se entrega al receptor una notificación. El receptor debe ir a la unidad FortiMail para abrir el mensaje. La unidad FortiMail almacena el mensaje.
- *Encryption algorithm*: algoritmo de cifrado que se usará para el cifrado del email. Cuando la unidad opera en modo de operación seguro, únicamente permite: AES 128, AES 192, AES 256.
- *Action on failure*. Acción que la unidad FortiMail llevará a cabo cuando el cifrado del mensaje no se pueda realizar:
  a) *Drop and send DSN*: enviar una notificación de estado de entrega (DSN) a la dirección de correo del emisor, indicando que el email no ha sido entregado.
  b) *Send plain message*: entregar el email sin cifrar.
  c) *Enforce TLS*:
     1. Si la regla de entrega de mensajes (*delivery rule*) tiene un Perfil TLS configurado y este es de tipo *Encrypt* o *Secure*, la unidad FortiMail no hará nada más, ya que este perfil TLS ya hace que la unidad *FortiMail* fuerce el establecimiento de una conexión TLS con el receptor del email.
     2. Si la regla de entrega de mensajes (*delivery rule*) no tiene ningún Perfil TLS configurado o sí, pero este es de tipo *None* o *Preferred* (lo cual no fuerza ninguna conexión TLS), la unidad FortiMail forzará el perfil TLS a tipo *Encrypt*, lo que establecerá una conexión TLS de forma obligatoria con el receptor del mensaje.

120. El comportamiento del servicio IBE de la unidad FortiMail deberá configurarse desde *Encryption > IBE > IBE Encryption*, y los usuarios que utilizarán este servicio, deberán configurarse desde la opción *Domain & User > IBE User*. Para más información acerca del uso de IBE, consultar el Apartado "*Configuring IBE encryption*" (página 541), de la Guía de Administración de FortiMail [REF1].

6.7.2 PERFIL DE CIFRADO S/MIME

121. El estándar S/MIME se puede usar para firmar y/o cifrar correos electrónicos.

122. El perfil de cifrado S/MIME se configura desde *Profile > Security > Encryption*, seleccionando *Protocol: S/MIME*. Los parámetros a rellenar son similares a los indicados en el apartado anterior, salvo que la *IBE Action* se sustituye por *S/MIME Action*: Firmar, Cifrar o Firmar y cifrar.

123. Además, en el caso de S/MIME, es requisito que se hayan configurado previamente los "*Certificate Bindings*" correspondientes, que establecerán la relación entre una dirección o dominio de correo, y un certificado que prueba la identidad y proporciona las claves para el cifrado y/o firma.

124. Respecto al **cifrado de mensajes**:

- ***Recepción***: cuando llega un correo cifrado a la unidad FortiMail, esta compara la identidad del receptor, con su lista de *certificate bindings* para determinar si dispone de la clave para descifrar el mensaje. Si la encuentra, la utilizará para descifrar el mensaje y lo entregará descifrado. Si no, entregará el mensaje cifrado al receptor.
- ***Envío***: si la unidad FortiMail tiene que entregar un mensaje y tiene configurada una regla de entrega (*delivery rule*) con un perfil de cifrado S/MIME configurado con acción de cifrado, la unidad FortiMail compara la identidad del receptor con su lista de *certificate bindings* para determinar si dispone de la clave con la que cifrar el mensaje. Si encuentra la clave, la utilizará para cifrar el mensaje usando el algoritmo de cifrado especificado en el perfil S/MIME. Si no, realiza la acción configurada como *failure action* en dicho perfil.

125. Respecto a la **firma de mensajes:**

- ***Recepción***: cuando llega un correo con una firma electrónica a la unidad FortiMail, esta no verificará la firma, sino que lo entregará al receptor que es quien realizará la verificación de firma.
- ***Envío***: si la unidad FortiMail tiene que entregar un mensaje y tiene configurada una regla de entrega (delivery rule) con un perfil de cifrado S/MIME configurado con acción de firma, la unidad FortiMail compara la identidad del receptor con su lista de *certificate bindings* para determinar si dispone de un certificado y de una clave (privada) con la que firmar el mensaje. Si la encuentra, la utilizará para generar una firma que añade al mensaje, usando el algoritmo de firma especificado en el perfil. Si no, realiza la acción configurada como *failure action* en dicho perfil.

126. Los "*certificate binding*" se configuran desde *Encryption > S/MIME > Certificate Binding*. Para más información, consultar el Apartado "Configuring certificate bindings" (página 546) de la Guía de Administración de FortiMail [REF1].

127. Para más información acerca del uso de cifrado S/MIME, consultar el Apartado "*Using S/MIME encryption*" (página 486) de la Guía de Administración de FortiMail [REF1].

6.8 AUTENTICACIÓN DE CONEXIONES SMTP

128. Las reglas de control de acceso (*Access Control Rules*) son las que gobiernan las conexiones SMTP. Se categorizan en función de si las reglas aplican a la recepción o al envío de mensajes por parte de la unidad FortiMail, es decir, en función de si la unidad FortiMail es la destinataria o la iniciadora de la sesión SMTP.

129. Las reglas de control de acceso que aplican a la recepción de mensajes determinan si la unidad FortiMail va a procesar y entregar, rechazar o descartar los mensajes de correo para las sesiones SMTP iniciadas por los clientes SMTP.

130. Para que la unidad FortiMail solo acepte conexiones de clientes SMTP autenticados, las correspondientes reglas de control de acceso deben tener como obligatoria la autenticación (*Authentication Status = Authenticated).* **Se debe verificar que no existan reglas de control de acceso que permitan conexiones no autenticadas.** Para ello:

a) Deben instalarse los correspondientes certificados de servidor, cliente y de las CAs (ver apartado 6.5 GESTIÓN DE CERTIFICADOS).

b) Debe habilitarse SMTP sobre TLS (SMTPS) en las opciones de configuración globales del servidor desde *System > Mail Settings > Mail Server Settings*.

c) Debe asignarse un perfil TLS a la regla de control de acceso (ver apartado 6.6 PERFILES TLS).

131. Respecto al envío de mensajes, las reglas de entrega de mensajes (*Delivery Rules*) aplican a las sesiones SMTP iniciadas por la unidad FortiMail con el objetivo de entregar mensajes de correo. Estas reglas se configuran desde *Policy > Access Control > Delivery* y permiten forzar el uso de TLS para las sesiones SMTP usando los TLS Profiles (ver apartado 6.6 PERFILES TLS). También permiten aplicar cifrados S/MIME o IBE asignando un Perfil de Cifrado (ver apartado 6.7 PERFILES DE CIFRADO IBE Y S/MIME).

132. **No se recomienda crear ninguna regla de control de acceso cuyo *Sender pattern* sea: *, *Recipient pattern* sea *, *Authentication status* sea *Any*, *TLS profile* sea None, y *Action* sea Relay**. Esta regla haría match con todas las conexiones y entregaría todos los mensajes (*open relay*) lo que podría resultar en que nuestro dominio protegido entre en Listas negras.

133. Para más información a este respecto, se recomienda consultar el apartado "*Configuring Access control rules*" (página 363) de la Guía de Administración de FortiMail [REF1].

6.9 SINCRONIZACIÓN

134. La sincronización de fecha y hora de los componentes de un sistema es muy importante para asegurar que los logs tienen un correcto "*timestamp*". La configuración de un servidor NTP no está contemplada para una configuración segura del producto, por lo que se mantendrá la fecha y hora del reloj del sistema

proporcionadas por el *hardware* como referencia, las cuales podrán ser establecidas manualmente desde el apartado *System > Configuration > Time*.

6.10 ACTUALIZACIONES

6.10.1 ACTUALIZACIÓN DE FIRMAS Y MOTORES DE INSPECCIÓN

135. **Se debe llevar a cabo la actualización automática de firmas y motores de inspección antivirus al menos una vez al día**. Los comandos son los siguientes:

```
config system fortiguard antivirus
  set scheduled-update-frequency daily
  set scheduled-update-status enable
  set scheduled-update-time <time_str>
end
```

136. Es necesario indicar que es requisito previo contar con una suscripción al servicio FortiGuard Antivirus y/o FortiGuard anti-spam. El proceso de actualización también se puede llevar a cabo desde la interfaz web, desde la opción *System > FortiGuard > Antivirus*, desde la que se puede configurar la dirección IP del servicio FortiGuard, los parámetros relativos a la planificación de las actualizaciones, y la posibilidad de programarlas de forma automática, o para su realización de manera manual.

137. Para más información acerca del proceso de actualización de firmas antivirus, ir al apartado "*Configuring FortiGuard Services*" (página 288) de la Guía de Administración de FortiMail [REF1].

6.10.2 ACTUALIZACIÓN DEL *FIRMWARE* DEL DISPOSITIVO

138. El comando *get system status* se emplea desde el CLI para obtener la versión instalada de *firmware*, así como otra información relevante.

139. Al iniciar el proceso de actualización del *firmware*, la unidad FortiMail hace una verificación automática de la firma que contiene el fichero de *firmware*. El proceso de actualización por parte de un administrador es descrito a continuación:

- El administrador descarga la actualización desde la página de soporte de Fortinet [REF13].
- El administrador procederá a copiar dicho archivo a la unidad FortiMail empleando un canal de confianza como la interfaz web, que emplea el protocolo HTTPS.
- El administrador debe verificar que el valor MD5 del fichero de firmware coincide con el indicado en la web de FortiMail.

140. El proceso de actualización se realiza de la misma forma que el proceso de instalación indicado en el apartado 5.2 INSTALACIÓN SEGURA sobre la Instalación Segura. Se describe el procedimiento en la documentación de la unidad FortiMail

en el apartado "*Installing Firmware*" (página 578) de la Guía de Administración de FortiMail [REF1].

141. En caso de que la carga del nuevo *firmware* falle, se mostrará un mensaje de error. La potestad de llevar a cabo actualizaciones se limita a los administradores de seguridad.

6.11 AUTO-CHEQUEOS

142. Durante el arranque del dispositivo se realizan automáticamente una serie de test de integridad del *firmware* y de los mecanismos criptográficos (test KAT, *Known Answer Test*), que se pueden visualizar desde la consola:

- Test de integridad de *firmware*.
- Test de Bypass de configuración con HMAC SHA-256.
- AES, CBC mode (KAT).
- AES, GCM mode (KAT).
- HMAC SHA-1 (KAT).
- SHA-1 (KAT).
- SHA-256 / HMAC SHA-256 (KAT).
- SHA-384 / HMAC SHA-384 (KAT).
- KAT de Generación y verificación de firma RSA.
- Test del DRBG.

143. En caso de que todos los tests sean completados con éxito, se observará el siguiente mensaje:

```
Self-tests passed.
```

144. En el caso de fallo de alguno de los chequeos, el dispositivo inmediatamente procederá al apagado.

```
Self-tests failed Entering error mode...
The system is going down NOW!!
The system is halted
```

145. En caso de entrar en modo de error tras fallar alguno de los tests, el producto entrará en un estado seguro que no permitirá el paso de ningún tipo de dato.

146. **Se debe ejecutar el auto-chequeo de forma periódica** para verificar que no hay ningún problema en el dispositivo. Para ello, se debe utilizar el siguiente comando:

```
execute fips kat { aes | configuration-test | integrity-test | rng | rsa | sha1-hmac}
```

147.En caso de seleccionar all, se realizarán todos los auto-chequeos:

```
execute fips kat all
```

6.12 ALTA DISPONIBILIDAD

148.La configuración de Alta Disponibilidad puede ser de dos (2) tipos: Activo-Activo o Activo-Pasivo.

Activo-Activo:

- Todos los equipos prestan el servicio, por lo que maximiza y prioriza el rendimiento repartiendo la carga entre las distintas unidades que formen parte del clúster, llegando a un máximo de 25 dispositivos.
- La configuración activa [REF8] es idéntica en todas las unidades, por lo que, en caso de indisponibilidad de cualquiera de ellas, otro miembro puede ofrecer el mismo nivel de servicio con garantías. Este chequeo se realiza mediante el cálculo de "*checksums*" por configuración, de modo que cualquier discrepancia será notificada.
- Para este tipo de despliegues se puede utilizar registros MX ("*Mail Exchanger*") con una misma prioridad (el dominio se resuelve con múltiples IPs) o un balanceador de carga que permitirá una aproximación más precisa, ofreciendo distintos algoritmos de elección de miembro basados en el rendimiento, calidad o respuesta de cada uno de los nodos.
- Ya que sólo la configuración está replicada entre todas las unidades, en caso de indisponibilidad, la información de archivo y cuarentena (en caso de no utilizar un almacenamiento externo como una NAS) puede perderse.

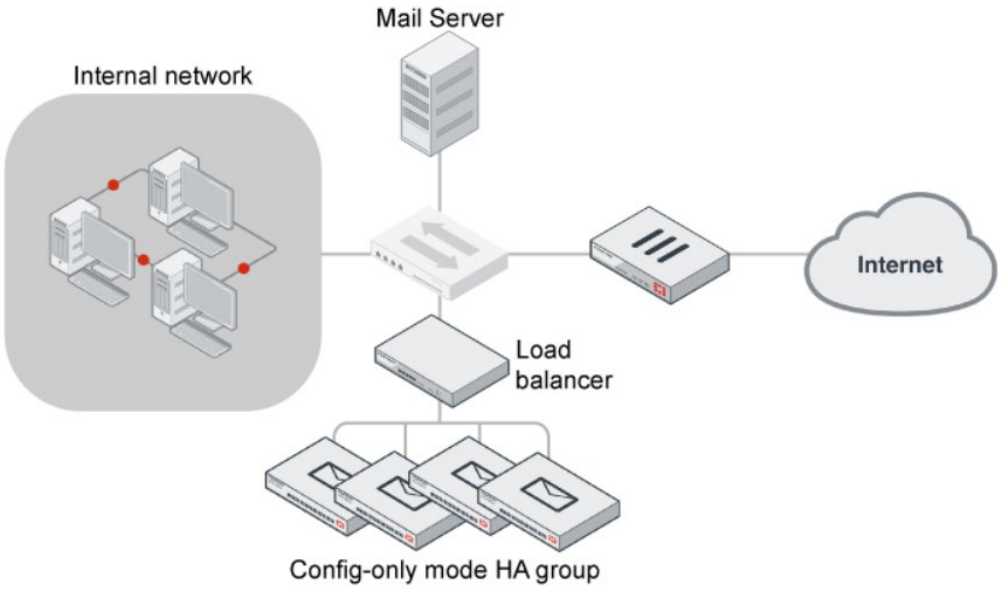


Figura 8. Arquitectura A-A

Activo-Pasivo:

- En esta configuración [REF9] se prioriza la disponibilidad formando un clúster de 2 unidades. Mientras una de ellas procesa toda la carga del servicio, la secundaria mantendrá chequeos de salud y sincronismo de configuración, ficheros y bases de datos.
- Si alguno de estos chequeos detecta indisponibilidad o algún comportamiento errático, el dispositivo inactivo, cambiará de rol pasando a asumir el servicio.
- Una vez más haciendo uso de "*checksums*" se garantiza, no sólo, la consistencia de configuración, sino también archivo, cuarentenas, etc., entre ambos nodos de modo que se pueda ofrecer el mismo nivel de servicio con cualquiera de ellos.
- A diferencia del anterior modelo donde sólo se extiende la configuración activa, en caso de fallo de uno de los dispositivos no hay pérdida de información. En todos los aspectos, ambos equipos son "idénticos".
- Otra ventaja a tener en cuenta es que no es necesario depender de mecanismos de balanceo adicionales.

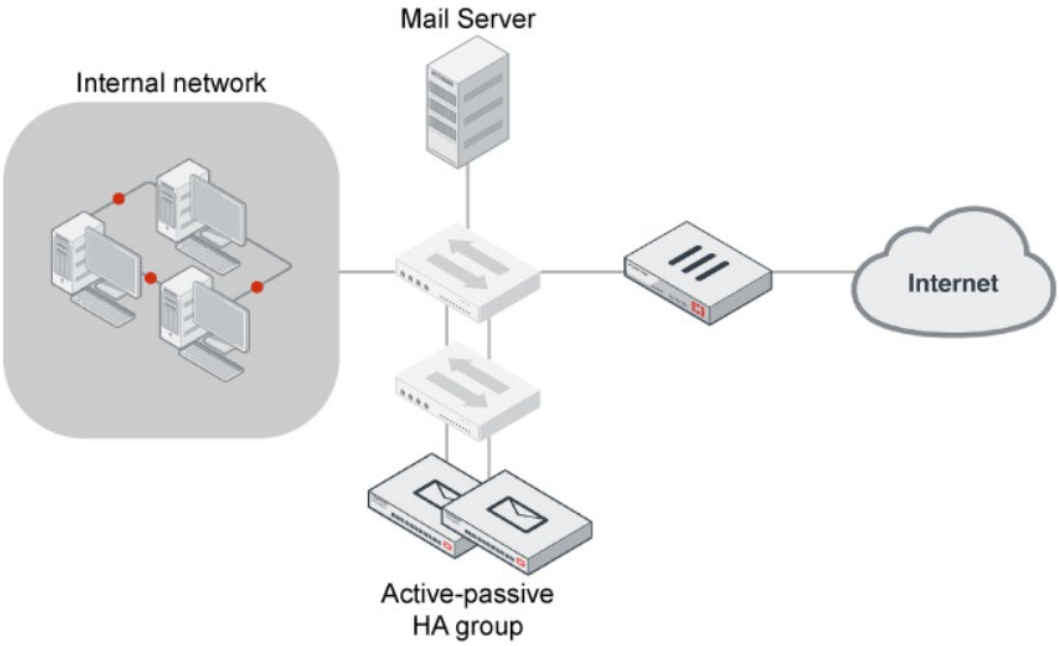


Figura 9. Arquitectura A-P

149. Para más información sobre Alta Disponibilidad, consultar el apartado "*Using High Availability (HA)*" (página 237) de la Guía de Administración de FortiMail [REF1].

6.13 AUDITORÍA

150. FortiMail permite registrar y visualizar cualquier actividad, tanto de rendimiento como de protección en el propio interfaz gráfico de la solución (WebUI). Este histórico puede llegar a ser hasta de 4 años dependiendo de las limitaciones físicas de la plataforma y su almacenamiento local, pudiéndose también reenviar estos datos a un servidor de informes y/o syslog externo, como FortiAnalyzer, o incluso, incorporar información a otros dispositivos del Security Fabric, como FortiSandbox o Fortigate.

151. Con la configuración de fábrica, FortiMail provee informes genéricos desde distintos puntos de análisis (*Top Sender, Top Spammer IP, Top Spam Type*...) generados a partir de registros. La creación de informes se puede programar y enviar automáticamente por correo. Se puede también utilizar FortiAnalyzer como servidor de log extendido de FortiMail, agregando informes más avanzados cuando los registros coinciden con algunos patrones.

152. La búsqueda de logs y el identificador de directivas facilitan el proceso de seguimiento de las actividades de correo y de identificación de las reglas aplicadas en un mensaje dado. La búsqueda cruzada de logs proporciona una correlación rápida entre registros de diferentes módulos. Por ejemplo, el administrador puede querer saber por qué exactamente un mensaje fue bloqueado. Gracias a la búsqueda cruzada, se obtendrá un análisis pormenorizado de todas las acciones realizadas por cada uno de los motores e incluso sobre el propio servicio.

153. El seguimiento de mensajes se simplifica al proporcionar una búsqueda de registro desde las colas de cuarentena y de correo. Para un mensaje determinado almacenado en FortiMail, se pueden recuperar fácilmente los detalles del clasificador y otros registros.

154. Al margen de este detalle, también existen distintos cuadros de mando predefinidos que ofrecen información útil de un solo vistazo y que nos dan una perspectiva global del funcionamiento de la plataforma, como ejemplos:

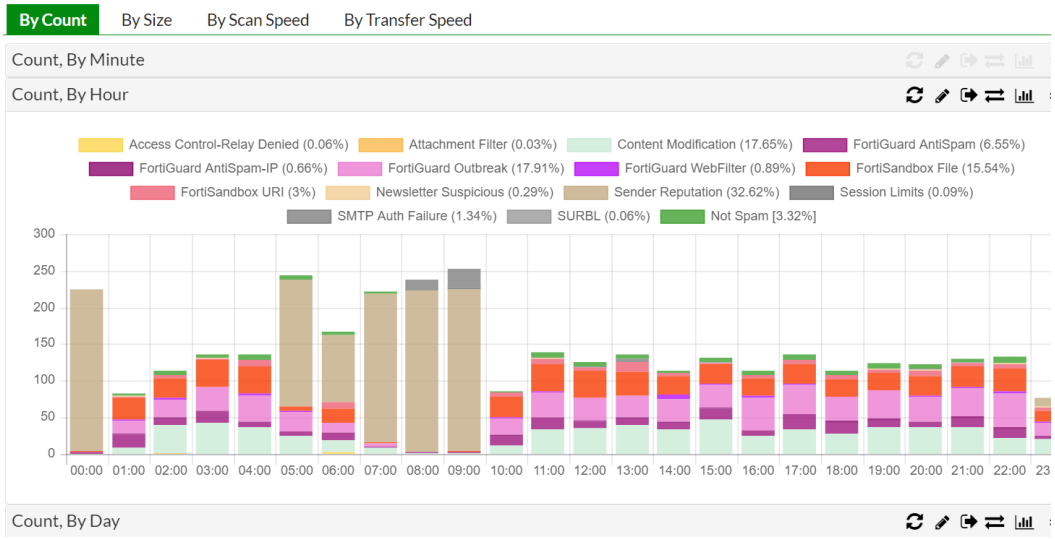


Figura 10. Cuadro de mando mostrando eventos de seguridad detectados en las últimas horas

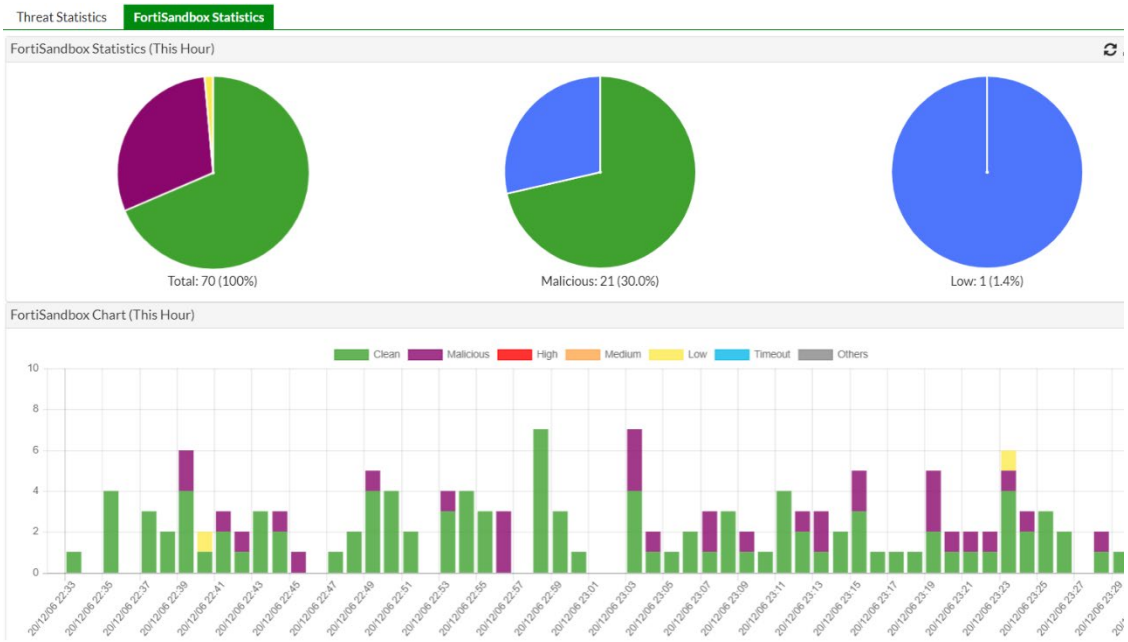


Figura 11. Estadísticas de eventos analizados con FortiSandbox

6.13.1 REGISTRO DE EVENTOS

155. La unidad FortiMail proporciona capacidades de registro de actividades relacionadas con virus maliciosos, incidentes de spam, y eventos del sistema, así como eventos relacionados con servidores de correo asociados y Webmail. Se puede seleccionar un umbral de severidad que los eventos deben alcanzar para ser almacenados en archivos de log.

156. A continuación, se muestra la sintaxis que siguen los mensajes de log. Todos los mensajes de log de FortiMail están compuestos por una cabecera y un cuerpo.

- **Cabecera:** contiene la fecha y hora en la que el log se originó, un identificador de log, el tipo de log, el nivel de severidad (prioridad), y donde se originó el mensaje.
- **Cuerpo:** describe la razón por la que el mensaje de log fue creado, así como las acciones emprendidas por la unidad FortiMail para responder al evento en cuestión.

157. Para más información acerca de la sintaxis de los archivos de log de FortiMail, consultar el apartado "*Log message syntax*" (Página 561) de la Guía de Administración de FortiMail [REF1].

158. Asimismo, para más información sobre los tipos de mensajes de log que la unidad FortiMail puede registrar, consultar el apartado "*FortiMail log types*" (página 562) de la Guía de Administración de FortiMail [REF1].

6.13.2 ALMACENAMIENTO LOCAL Y REMOTO

159. Una unidad FortiMail puede ser configurada para almacenar logs de forma local o remota (enviarlos a un servidor *syslog* o a una unidad FortiAnalyzer), o en ambas localizaciones a la vez. Estos archivos de log pueden ser visualizados y descargados desde *Monitor > Log*.

160. Cuando un fichero de log alcanza el límite de tamaño o antigüedad, la unidad FortiMail procede a rotar el fichero de log actual. Para ello, renombra dicho archivo con un nombre que indica su relación secuencial con respecto a otros archivos de log del mismo tipo, y a continuación crea un nuevo archivo de log vacío.

161. A continuación, se introducen los pasos a seguir para almacenar los logs en local:

1. Ir a *Log and Report > Log Settings > Local.*
2. Seleccionar la opción *Enable*, para permitir el almacenamiento de los logs en el disco duro.
3. En *Log file size*, introducir el límite de tamaño para el fichero de logs actual, en megabytes (MB).
4. En *Log time*, introducir el período de tiempo (en días) de antigüedad permitida para los archivos de log. El rango válido se sitúa entre 1 y 366 días.
5. En *Hora*, introducir la hora del día (en formato 24 horas) en la que se producirá la rotación de los archivos de log.
6. En *Log level*, seleccionar la severidad que un log deberá alcanzar o superar para ser almacenados.
7. En *Log retention period*, especificar el período de tiempo por el que los logs serán conservados. El rango válido se sitúa entre 0 y 1461 días. 0 implica que no hay límite de tiempo.
8. Seleccionar la acción a realizar cuando el disco duro local está lleno, y llega un nuevo mensaje de log. Las opciones disponibles son “no almacenar” (do not log) o “sobreescribir”.
9. En *Logging Policy Configuration*, habilitar los tipos de log que se desea almacenar en el almacenamiento local.
10. Hacer click en *Apply*.

162. **Es recomendable configurar el envío y almacenamiento de logs en un servidor remoto**, por ejemplo, un *appliance FortiAnalyzer*, un servidor syslog o un SIEM (ya que es compatible con formato CEF). Para que la comunicación entre el producto y el dispositivo externo se lleve a cabo con éxito, es necesario permitir el tráfico en todos los cortafuegos intermedios que puedan existir con los puertos adecuados. En el caso de syslog, el puerto es el 514/UDP por defecto, aunque se recomienda y soporta el intercambio TCP.

163. A continuación, se introducen los pasos a seguir para enviar los logs [REF6]:

a) Ir a *Log and Report > Log Settings > Remote.*

b) Hacer click en *New* para crear una nueva entrada, o hacer doble click en una entrada existente para modificarla.

c) Seleccionar *Enable* para permitir el envío de logs a un host remoto.

d) En *Profile name*, introducir un nombre para el perfil.

e) En *IP*, introducir la dirección IP del servidor syslog o de la unidad FortiAnalyzer en que la unidad FortiMail almacenará los logs.

f) En *Port*, si el host remoto es una unidad FortiAnalyzer, introducir el valor 514; si el host remoto es un servidor syslog, introducir el puerto en el que dicho servidor se encuentra a la escucha.

g) En *Level*, seleccionar el nivel de severidad que un mensaje de log debe igualar o superar para ser almacenado en el servidor externo.

h) En *Facility*, seleccionar el identificador que la unidad FortiMail usará para identificarse a sí mismo a la hora de enviar mensajes de log.

i) Habilitar el formato CSV en caso de querer enviar los logs en formato CSV.

j) En *Log protocol*, seleccionar el protocolo que utilizará la unidad FortiMail para el envío de logs. Admite dos (2) protocolos: **syslog** y **OFTPS**. **Se recomienda el uso de FortiAnalyzer como servidor remoto de auditoría dado que la comunicación con el servidor syslog no ha sido evaluada**, en cuyo caso el protocolo que se utilizará por defecto es OFTPS (Optimized FTPS). Se trata de FTP sobre TLS. En la unidad FortiMail deberá seleccionarse OFTPS en *Log Protocol*, y seleccionar el algoritmo HASH (SHA256 es el valor recomendado). En la unidad **FortiAnalyzer se configurarán el resto de parámetros de la conexión, como la versión TLS 1.2 y los algoritmos criptográficos a usar en el protocolo, que deberán ser de los autorizados en la CCN-STIC-807 para nivel Alto de ENS.**

k) En *Logging Policy Configuration*, habilitar los tipos de logs que se desea almacenar en el servidor remoto.

l) Hacer click en *Create*.

164. A continuación, se introducen los comandos necesarios para configurar la conexión a un dispositivo FortiAnalyzer a través del CLI:

```
config system fortiguard antivirus
  edit <identificador>
    set status enable
    set server <IP_FortiAnalyzer>
    set event-log-status enable
end
```

Donde:

- *<identificador>:* será un identificador numérico que se asociará al servidor remoto que se está configurando.
- *<IP_FortiAnalyzer>:* será la dirección IP de la unidad FortiAnalyzer que recibirá los logs procedentes de la unidad FortiMail.

165. Para más información sobre el proceso a seguir para enviar los logs a un servidor syslog externo o a una unidad FortiAnalyzer, consultar el apartado *"Configuring logging to a syslog server or FortiAnalyzer unit"* (página 569), de la Guía de Administración de FortiMail [REF1].

6.14 BACKUP

166. Antes de llevar a cabo cualquier intervención que suponga una modificación en el equipo, **es recomendable realizar un "*backup*" de la configuración**, de modo que ante un problema se pueda recuperar el sistema cargando la configuración anterior a la modificación realizada.

167. Los backups realizados podrán almacenarse, tanto en el equipo de administración, como en dispositivos externos ("*off-site*").

168. Tanto por CLI como por GUI se puede configurar la realización de *backups* con la cadencia necesaria, tanto en local con gestión de versiones, como en remoto. En la siguiente imagen correspondiente al menú *System > Maintenance > Configuration* se muestran las diferentes capacidades de esta característica:

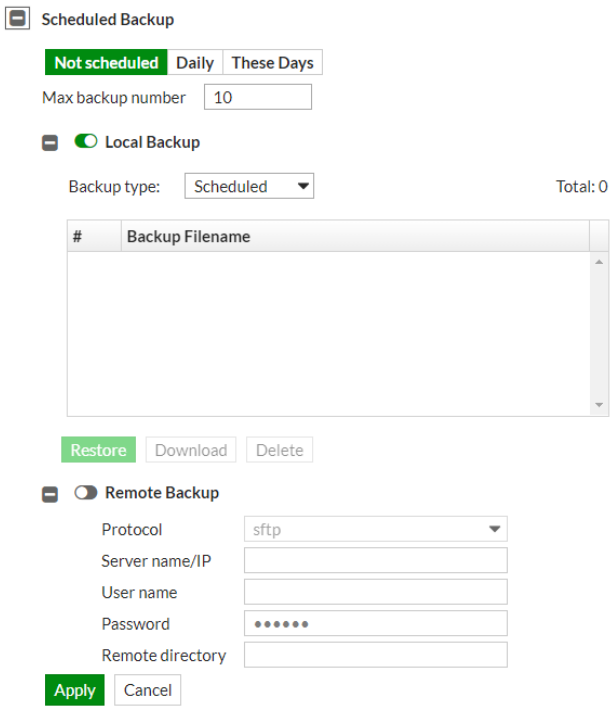


Figura 12. *Backups* programados

169. Aunque FTP está soportado (no recomendado), para una configuración segura **debe utilizarse SFTP** en este intercambio. En el caso de realizarlos en local, el histórico de

configuraciones estará disponible para ser recuperado si fuese necesario directamente con el botón *Restore*.

170. Asimismo, se puede forzar el backup en cada cierre de sesión de administrador con la siguiente variable:

```
config sys global
  set revision-backup-on-logout enable
end
```

171. Para llevar a cabo el *Restore*, se utilizará una copia de seguridad de la configuración desde un equipo local, usando el CLI o la interfaz web (UI).

172. A continuación, se enumeran los pasos necesarios para llevar a cabo la restauración de la configuración desde la interfaz web:

- Limpiar la caché del navegador web. En caso de que el navegador esté mostrando la interfaz web, refrescar la página.
- Realizar el *login* en la página del interfaz web.
- En el modo de gestión avanzada (*advanced management mode*), ir a *System > Maintenance > Configuration.*
- Hacer click en *Restore Configuration* para localizar y seleccionar el archivo de configuración que se desea restaurar. A continuación, hacer *click* en *Restaurar*.
- La unidad FortiMail procederá a restaurar la configuración, y a continuación se reiniciará.
- Una vez completada la restauración de la configuración, se recomienda verificar que todas las configuraciones han sido cargadas con éxito. Para más detalles sobre la verificación de la restauración de la configuración, consultar el apartado “Verifying the configuration” (página 582), de la Guía de Administración de Fortimail [REF1].

173. Solo es posible realizar la restauración mediante un servidor TFTP. A continuación, se enumeran los pasos necesarios para llevar a cabo la restauración de la configuración desde el CLI:

1. Iniciar una conexión desde el equipo de gestión a la consola local (CLI) de la unidad FortiMail, identificándose como el usuario *admin*, o una cuenta de administración que cuente con permisos de lectura y escritura.
2. Conectar la interfaz de red de la unidad FortiMail directamente al servidor TFTP o en la misma subred que este.
3. Copiar la copia de seguridad que se desea restaurar al directorio raíz del servidor TFTP.
4. Verificar que el servidor TFTP se encuentra funcionando, y que la unidad FortiMail tiene conectividad con el mismo. La conectividad se puede comprobar mediante el siguiente comando:

Execute ping <IP_TFTP_server>

5. Introducir el siguiente comando:

Execute restore config tftp <file_name> <tftp_ipv4>

6. Se mostrará el siguiente mensaje:

This operation will overwrite the current settings! (The current admin password wull be preserved.) Do you want to continue? (y/n)

7. Introducir el carácter *y*. La unidad FortiMail restaurará la configuración, y se reiniciará.

174. Una vez completada la restauración de la configuración, se recomienda verificar que todas las configuraciones han sido cargadas con éxito. Para más detalles sobre la verificación de la restauración de la configuración, consultar el apartado "*Verifying the configuration*" (página 582), de la Guía de Administración de Fortimail [REF1].

6.15 BORRADO SEGURO

175. Se permite llevar a cabo el formateo del almacenamiento *flash* del dispositivo, para lo relacionado con las claves de actualización e integridad del *firmware*, configuración de claves de cifrado y claves de conexión HTTPS/TLS. A continuación, se incluye el comando a ejecutar para llevar a cabo el formateo.

Execute erase-disk <bootdevice>

6.16 ANTI-SPAM

176. La funcionalidad principal de los dispositivos Fortimail es detectar correos electrónicos ilícitos, ya sea porque no se ajustan al formato esperado o por su contenido, en las distintas fases de recepción o envío, y, por tanto, clasificables como SPAM.

177. El proceso de detección de spam consta de diferentes fases:

- **Fase de inspección durante la conexión:** al recibir la conexión desde un servidor de correo remoto, se inspeccionará si el origen del mensaje pertenece a una lista de mala reputación, o si ha alcanzado el número máximo de conexiones permitidas para el mismo.
- **Fase de inspección de las cabeceras:** una vez que se haya recibido el mensaje, se inspeccionará la cabecera del mismo para determinar si se trata de un

mensaje ilícito o no. Para ello, se realizará una serie de verificaciones sobre el remitente, cumplimiento con las RFC correspondientes, etc.

- **Fase de inspección del contenido:** en esta fase se llevará a cabo el análisis del contenido del mensaje, en busca de posibles virus o *malware*, o algún tipo de código malicioso incrustado en dicho contenido, ya sea en el texto del mensaje, en imágenes, o en código embebido en el mismo o en ficheros adjuntos.

6.16.1 DOMINIOS DE PROTECCIÓN

178. La configuración de dominios permite indicar al dispositivo los correos sobre los que llevar a cabo la inspección. Esta configuración se realiza en base al nombre de dominio contenido en la dirección de correo electrónico.

179. La configuración de los dominios se lleva a cabo desde la opción *Domain & User > Domain > Domain.*

180. Para más información sobre la configuración de dominios de protección, dirigirse al apartado "*Configuring Domains and Users*" (página 307) de la Guía de Administración de FortiMail [REF1].

6.16.2 PERFILES

181. Los perfiles permiten la configuración de los posibles métodos de análisis de correos electrónicos, cuando estos son seleccionados en una política, permitiendo de esta forma aplicar el perfil a todos los mensajes de correo y conexiones SMTP gobernados por la política.

182. Los perfiles se configuran desde la opción *Profile*. Hay distintos perfiles, correspondientes a las diferentes fases de la inspección de un correo electrónico, y pueden ser configurados tanto para el correo electrónico saliente, como para el entrante. A continuación, se enumeran algunos de estos perfiles:

- **Perfil de Sesión:** Los perfiles de sesión se centran en la conexión y el envoltorio de la sesión SMTP. Permiten, entre otras opciones, controlar el número de conexiones y mensajes por cliente, *timeouts* de sesión, llevar a cabo la validación del emisor, rechazar comandos SMTP si estos son sintácticamente incorrectos, etc.

  La configuración de los perfiles de sesión se puede consultar con detalle en el apartado "*Configuring session profiles*" (página 390), de la Guía de Administración de Fortimail [REF1].

- **Perfil *anti-spam*:** los perfiles *anti-spam* representan un conjunto de técnicas de escaneo, que se aplicarán sobre los mensajes de correo. Estas técnicas de escaneo comprenden las técnicas propias de la unidad FortiMail, así como las proporcionadas por el servicio anti-spam de FortiGuard. El servicio proporcionado por *FortiGuard* proporciona tres (3) elementos para la detección de spam: listas de bloque DNS (DNSBL), escaneado en profundidad basado en URIs (*Uniform Resource Identifier*) contenidas en el cuerpo del mensaje, y

FortiGuard anti-spam Spam *Checksum Blocklist* (SHASH), que compara los hashes de mensajes enviados por FortiMail, con hashes de mensajes de spam conocidos.

Cuando el perfil anti-spam determina que un mensaje de correo es spam, la acción por defecto es marcarlo como tal, y dejarlo en cuarentena (almacenado en la unidad FortiMail). Existen otras opciones posibles, como rechazar el mensaje y notificar al emisor, descartar el mensaje sin ningún tipo de aviso al emisor, etc.

La configuración de los perfiles anti-spam se puede consultar con detalle en el apartado "*Configuring antispam profiles and antispam action profiles*" (página 410), de la Guía de Administración de Fortimail [REF1].

- **Perfil de contenido**: En el apartado 7.7.1 PERFILES DE CONTENIDO Y DICCIONARIO se trata en detalle la información asociada a estos perfiles.

  La configuración de los perfiles de contenido se puede consultar en el apartado "*Configuring content profiles and content action profiles*" (página 432), de la Guía de Administración de Fortimail [REF1].

6.16.3 POLÍTICAS

183. Las políticas definen el modo en que se filtrará el tráfico de la unidad FortiMail. También permiten definir aspectos de la configuración de cuentas de usuario, como el tipo de autenticación, configuración de acceso a correo web, etc. Tras la creación de los diferentes perfiles mencionados con anterioridad en este documento, estos deben ser aplicados a la política correspondiente para que tengan efecto. A continuación, se enumeran brevemente los tipos de políticas ofrecidas por FortiMail. Las políticas se configuran desde la opción *Policy*, siendo estas:

    - **Políticas de Control de Acceso**: Determinan las reglas de control de acceso para las sesiones SMTP (ver apartado 6.8 AUTENTICACIÓN DE CONEXIONES SMTP). Estas políticas se categorizan de forma separada, basándose en si afectan a la entrega o a la recepción de mensajes de correo, dependiendo de si la unidad FortiMail es la que inicia la sesión SMTP, o si la receptora de dicha sesión, iniciada por un cliente SMTP. Es necesario indicar que sólo una regla de control de acceso es aplicada sobre una determinada sesión SMTP.

    - **Políticas basadas en IP:** Se aplica en función de la dirección IP del cliente SMTP. Asimismo, se aplica también sobre el servidor SMTP cuando la unidad FortiMail opera en modo Transparente.

    - **Políticas basadas en el Receptor**: Este tipo de política aplicará en función del dominio de la dirección de correo del destinatario del mensaje.

184. Se puede consultar información en detalle sobre la configuración y uso de las políticas en el apartado "*Configuring policies*" (página 362), de la Guía de Administración de Fortimail [REF1].

7. FUNCIONALIDADES DE SEGURIDAD

7.1 FORTIGUARD *ANTI-SPAM*

185. El servicio anti-spam FortiGuard es un servicio administrado por Fortinet que proporciona un enfoque de tres (3) elementos para la detección de mensajes de correo electrónico con contenido dañino:

- Lista de Bloques DNS (DNSBL): lista "activa" de orígenes de spam conocidos.
- Filtrado de correo electrónico detallado basado en un identificador uniforme de recursos (URI): incluido en el cuerpo del mensaje, comúnmente conocido como listas de agujeros reales (SURBL) URI de spam.
- Función FortiGuard anti-spam Checksum Blocklist (SHASH): Mediante SHASH, la unidad FortiMail envía un hash de un correo electrónico al servidor anti-spam FortiGuard, que compara el hash con los hashes de los mensajes de correo basura conocidos almacenados en la base de datos anti-spam FortiGuard. Si los resultados del hash coinciden, el correo electrónico se marca como spam. Los filtros también se pueden configurar para clasificar ciertas clases de URI como spam, basándose en las mismas calificaciones que FortiGate (malintencionado, suplantación de identidad, etc). Es posible configurar una lista de identificadores URI que estén exentos de ser clasificados como spam.

186. A continuación, se describen las distintas **funcionalidades anti-spam proporcionadas por el producto, que deberán ser activadas**. Para ello, se debe activar en un perfil anti-spam y aplicar dicho perfil a una política, siguiendo los pasos:

- Ir a *Profile* > *AntiSpam* > *AntiSpam.* Hacer clic en *New*.
- Seleccionar el dominio en el que será de aplicación el perfil y asignarle un nombre identificativo.
- En la casilla *Default Action*, seleccionar la acción por defecto que se realizará.
- A continuación, en el listado de funcionalidades, activar las deseadas. Al lado de cada acción se puede seleccionar la acción concreta que realizará o dejar la acción por defecto (ver apartado 7.2 ACCIONES ANTI-SPAM).
- Por último, hacer clic en *Ok*.

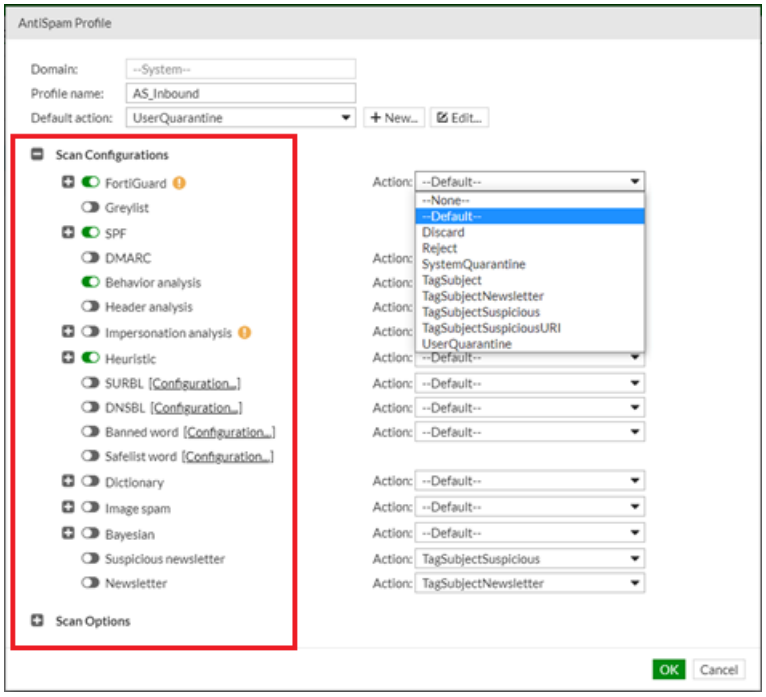


Figura 13. Configuración de funcionalidades Anti-spam

7.1.1 FORTIGUARD *ANTI-SPAM DNSBL (IP BLOCK)*

187. Para lograr una identificación actualizada en tiempo real, el producto utiliza sondas de spam distribuidas globalmente, que reciben más de un millón de mensajes de spam al día. Utiliza múltiples capas de procesos de identificación para producir una lista actualizada de orígenes de spam. Para mejorar el servicio y optimizar el rendimiento, el servicio anti-spam FortiGuard revisa continuamente cada una de las identidades conocidas de la lista para determinar el estado del origen (activo o inactivo).

188. Si un origen de spam conocido ha sido retirado del servicio, el servicio anti-spam FortiGuard elimina el origen de la lista, proporcionando así a los clientes precisión y rendimiento.

7.1.2 FORTIGUARD *ANTI-SPAM SURBL*

189. Para detectar el spam basado en los URIs del cuerpo del mensaje (normalmente sitios web), Fortinet utiliza la tecnología anti-spam FortiGuard SURBL. Como complemento del componente DNSBL, que bloquea los mensajes basados en el origen del spam, la tecnología SURBL bloquea los mensajes que tienen hosts de spam mencionados en los cuerpos de mensajes.

190. Al analizar el cuerpo del mensaje, SURBL puede determinar si el mensaje es un mensaje de spam conocido independientemente del origen. Esto mejora la tecnología DNSBL al detectar mensajes de spam de orígenes de spam que pueden ser dinámicos, o un origen de spam que aún no se conoce en el servicio DNSBL. La combinación de ambas tecnologías proporciona un servicio administrado superior

con tasas de detección más altas que las DNSBL tradicionales o las SURBL por sí solas.

7.1.3 BEHAVIORAL ANALYSIS

191. Los métodos de FortiGuard son buenos para detectar el contenido volumétrico de spam y el spam previamente visto de direcciones IP conocidas, pero los atacantes ajustan a menudo su comportamiento para evitar la detección, por ejemplo, usando IPs previamente limpias, pero ahora infectadas para distribuir spam y cambiar contenido ocultando texto aleatorio en el cuerpo del correo. FortiMail Behavioral Analysis utiliza una lógica difusa y un aprendizaje automático para buscar ataques que tienen características comunes a los mensajes de spam observados recientemente.

7.1.4 SPAM OUTBREAK PROTECTION

192. *Outbreak protection* es una técnica para detectar ataques nuevos. Para mejorar las posibilidades de detectar virus o spams desconocidos, la protección *outbreak* de FortiMail analizará los mensajes sospechosos dos veces antes de la entrega: una vez cuando se recibe el mensaje y otra vez después de un período de tiempo *outbreak* (configurable de 15 minutos a 6 horas). Durante ese período, la base de datos de FortiGuard se enriquece con nueva información y podría devolver un nuevo resultado del análisis.

7.1.5 IMPERSONATION ANALYSIS SCAN

193. Este método busca engañar a los usuarios enviando correos electrónicos que afirman ser de usuarios VIP o sensibles dentro de la organización. Se trata de enviar correos modificando el *Display Name* para engañar al usuario interno. Las asignaciones de direcciones válidas de los usuarios válidos se pueden identificar de varias maneras:

- **Carga manual:** basada en patrones o *wildcards*.
- **Autodescubrimiento dinámico** del flujo de tráfico.

7.1.6 FORGED IP SCAN

194. Cuando FortiMail recibe un mensaje de correo electrónico, convierte la dirección IP del remitente en un nombre de host canónico. A continuación, la unidad FortiMail compara todas las direcciones IP registradas oficialmente para ese nombre de host con la dirección IP del remitente. Si no se encuentra la dirección IP del remitente, la unidad FortiMail considera que la dirección IP y/o el nombre de host se han falsificado y trata el correo como spam.

7.1.7 *GREYLIST*

195. El análisis *greylist* bloquea el correo basura en función del comportamiento del servidor de envío, en lugar del contenido de los mensajes. Al recibir un correo electrónico de un servidor desconocido, la unidad FortiMail rechazará temporalmente el mensaje. Si el correo es legítimo, el servidor de origen intentará enviarlo de nuevo más tarde, en cuyo momento la unidad FortiMail lo aceptará. Los remitentes de correo basura rara vez intentan un reintento.

196. El *greylist* tradicional tiene su principal inconveniente: puede retrasar la entrega del primer correo electrónico de todos los usuarios externos. FortiMail implementa una función de exención automática que disminuye significativamente ese impacto. Solo el primer correo electrónico originado desde un dominio y de una misma IP sería cuestionado por la *greylist*.

7.1.8 *SPF SCAN*

197. Cuando un remitente intercambia información vía SMTP con Fortimail, el dispositivo analizará el dominio y buscará las entradas SPF (*Sender Policy Framework*) dentro de su registro DNS asociado. Dichas entradas contienen, entre otra información, la lista de MTAs (*Mail Transfer Agent*) permitidas para el envío, este sería el primer chequeo para verificar si es lícito. A continuación, se sigue analizando el resto de información obtenida. Si hay una discordancia, se podrá escoger la acción a ejecutar con el correo.

198. La granularidad de SPF (estándar empleado para la protección contra la falsificación de direcciones en el envío de correo electrónico) permite distintos veredictos basados en el comportamiento de este chequeo, que pueden ir desde un estado FAIL categórico (en este caso el correo electrónico recibido debería ser rechazado), pasando por un Error Temporal, hasta un estado neutral (este estado indica que no se sabe si las direcciones IP empleadas están clasificadas como autorizadas o no, pero se recomienda aceptar los correos electrónicos asociados). FortiMail tiene la capacidad de permitir escoger qué acción tomar para cada uno de estos supuestos.

7.1.9 *DMARC SCAN*

199. Una capa adicional al punto anterior es DMARC (Autenticación de Mensajes Basada en Dominios, Informes y Conformidad. Mecanismo de autenticación de correo electrónico). Este realiza comprobaciones adicionales sobre el mensaje basándose en SPF y su firma DKIM (*DomainKeys Identified Mail*). Este último mecanismo garantiza que el mensaje no se ha modificado en tránsito gracias a claves públicas dentro del registro DNS del dominio. DKIM utiliza criptografía de clave pública para permitir al origen firmar electrónicamente correos electrónicos legítimos, de manera que puedan ser verificados por los destinatarios. Esta combinación garantiza una tasa de acierto muy alta en la detección de correos fraudulentos, y es muy extendida entre los servidores de correo.

7.1.10 *DNSBL SCAN*

200. Además de poder contar con el servicio anti-spam de *FortiGuard DNSBL* de Fortinet, la BBDD puede ser alimentada con listas negras de spam con información procedente de servidores de terceros o incluso internos de la propia corporación, configurables en los distintos perfiles de anti-spam.

7.1.11 SURBL SCAN

201. Además de admitir el servicio FortiGuard anti-spam SURBL de Fortinet, la unidad FortiMail admite servidores de listas de URI de spam definidos por el administrador y de terceros. El administrador puede especificar qué servidores SURBL públicos utilizar como parte de un perfil anti-spam.

7.1.12 DEEP HEADER SCAN

202. La exploración profunda de encabezados implica dos (2) comprobaciones separadas. La comprobación de IP examina los campos recibidos del encabezado de correo electrónico. A continuación, la unidad FortiMail extrae cualquier URI o IP del encabezado y los pasa al servicio anti-spam FortiGuard, a los servidores DNSBL o SURBL para comprobar el spam. El análisis de encabezados examina el encabezado completo del mensaje en busca de características de correo no deseado.

7.1.13 BAYESIAN SCAN

203. El análisis bayesiano utiliza bases de datos para determinar si un correo electrónico es spam. Para que el escaneo bayesiano sea eficaz, las bases de datos deben ser formadas con spam conocido y mensajes de correo electrónico legítimo para entrenar el modelo matemático que pone a prueba los patrones. Para mantener su efectividad, se deben enviar falsos positivos y falsos negativos a la unidad FortiMail para que el escáner bayesiano pueda aprender de sus errores.

204. El escáner Bayesiano de FortiMail utiliza tres (3) tipos de bases de datos: personal, grupal y global. Las bases de datos personales están asociadas a usuarios individuales, la base de datos de grupo se aplica a todos los usuarios de un dominio y la base de datos global se aplica a todos los usuarios alojados en dominios definidos en la unidad FortiMail.

7.1.14 HEURISTIC SCAN

205. La unidad FortiMail incluye reglas que utilizan el filtro heurístico. Cada regla tiene una puntuación individual para calcular la puntuación total de un correo electrónico. Estas reglas se mantienen gracias a FortiGuard, con muestras de SPAM conocido. En el dispositivo, se establecerá un umbral límite superior e inferior para cada perfil anti-spam.

206. Para determinar si un correo electrónico es spam, el filtro heurístico examina un mensaje de correo electrónico y agrega la puntuación de cada regla que se aplica a

ese correo electrónico. Si el total es mayor o igual al umbral superior, el filtro clasifica el correo electrónico como correo basura, se podrá definir la acción a tomar. Si el total es menor o igual al umbral inferior, el correo electrónico no es spam. Si el total está entre los dos umbrales, el filtro heurístico no proporcionará un veredicto definitivo gracias a este motor. Tanto el umbral superior como el inferior pueden configurarse para obtener un resultado óptimo de falsos positivos o negativos.

7.1.15 DICTIONARY SCAN

207. El módulo de escaneo de diccionario permite al administrador definir diccionarios multilingües de palabras que no deben aparecer en el correo electrónico. Al aplicar ciertos pesos y umbrales, estos diccionarios se pueden utilizar para admitir la detección como spam. En este módulo también se aplica inteligencia al tener en cuenta parámetros como la distancia entre palabras claves que han hecho match, contexto, si forman parte del asunto u otros campos sensibles y otros métodos.

7.1.16 BANNED WORD SCAN

208. Se puede especificar una lista de palabras prohibidas como parte de un perfil anti-spam. Si la unidad FortiMail detecta cualquiera de las palabras prohibidas en el cuerpo o cabeceras del correo electrónico, marca el correo como spam.

7.1.17 NEWSLETTER

209. Permite la detección de boletines informativos. Puede que no sean spam, pero se pueden etiquetar con una palabra clave para facilitar la clasificación por el destinatario.

7.1.18 SUSPICIOUS NEWSLETTER

210. Similar a la detección de boletines, pero realiza comprobaciones adicionales para ver si el mensaje es realmente spam. Este veredicto viene dado también por el histórico de campañas y la reputación agregada de motores de análisis anteriores.

7.1.19 SAFELIST/BLOCKLIST

211. A nivel de sistema, dominio o usuario es posible configurar direcciones IP y direcciones de correo electrónico que están exentas de ser clasificadas como spam (*safe*) o siempre clasificadas como spam (*block*). Adicionalmente, al margen de los administradores, los usuarios pueden administrar su propia lista *Safe/Block* desde el portal de usuarios.

7.1.20 SAFELIST WORD SCAN

212. De manera similar, se puede especificar una lista segura de palabras como parte de un perfil *anti-spam*. Si la unidad FortiMail detecta una palabra en la lista blanca,

trata el mensaje como no spam y cancela el análisis anti-spam adicional. Este veredicto prevalece sobre el resto para la capa anti-spam, pero el resto de módulos (*AV, content, resources*) seguirán siendo analizados.

7.1.21 IMAGE SPAM SCAN

213. Los emisores de spam pueden intentar que sus mensajes de correo electrónico pasen las protecciones del spam reemplazando el cuerpo del mensaje con un archivo de imagen. Este archivo de imagen muestra un gráfico del texto deseado. Dado que el cuerpo del mensaje no contiene texto real, los escáneres diseñados para examinar el cuerpo del mensaje no encuentran nada con qué trabajar. Sin embargo, el escaneo de spam de imágenes de la unidad FortiMail está equipado para examinar e identificar gráficos GIF, JPEG y PNG utilizados en el spam de imágenes.

7.1.22 OTRAS OPCIONES

214. Los emisores de spam pueden adjuntar un archivo comprimido, un PDF o un documento de la suite de *Office* a un mensaje que de otra manera no sería válido. El archivo contendría información de spam. Dado que el cuerpo del mensaje no contiene texto, los motores anti-spam no pueden tener un veredicto claro. Habilitar la opción de análisis de ficheros de FortiMail aplica métodos heurísticos, escaneo de palabras prohibidas e imágenes spam sobre el contenido de archivos adjuntos.

215. Especificar el tamaño máximo del mensaje que se va a analizar (se puede establecer un tamaño ilimitado).

216. Evitar el análisis de spam para sesiones autenticadas.

217. Aplicar siempre la acción independientemente de la clasificación del mensaje.

7.2 ACCIONES ANTI-SPAM

218. Es posible asociar distintos sets de acciones a cada motor de spam, o de forma genérica que lo obtengan del set asociado al perfil (*default*). El comportamiento en caso positivo lo tomará del desplegable *Action*:

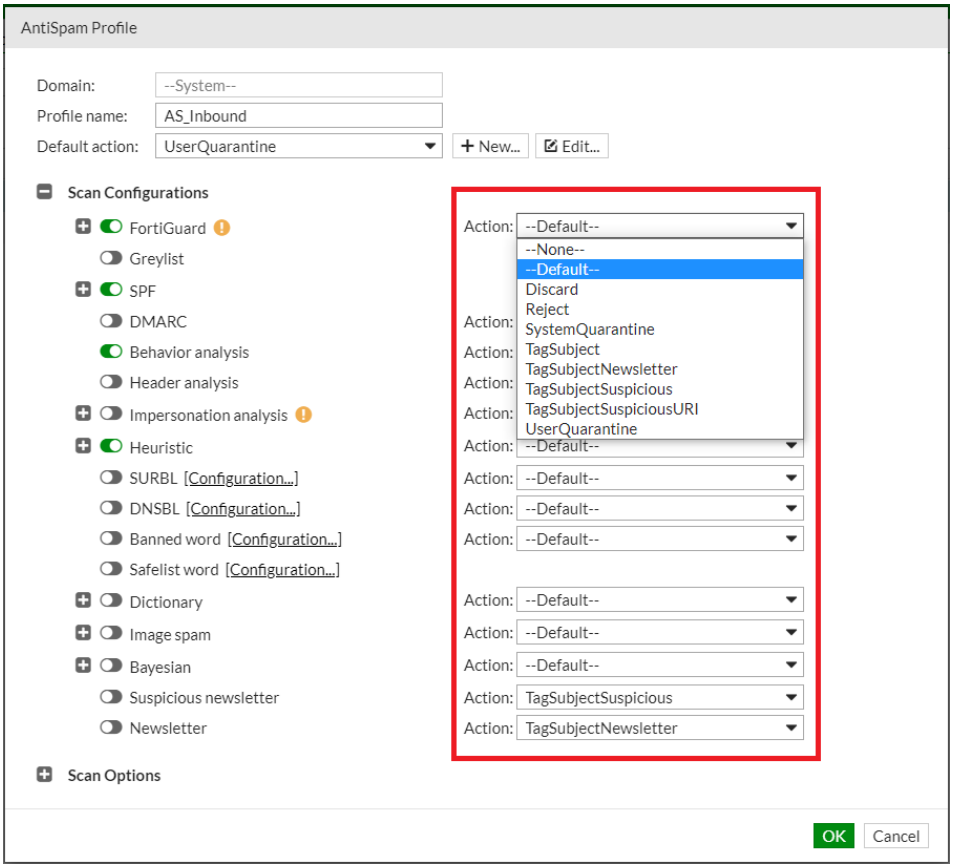


Figura 14. Valores de *action* por defecto para cada motor

219. Es posible personalizar nuevos sets de acciones simples o combinadas. Para ello se deben seguir los siguientes pasos:

1. Ir a *Profile* > *AntiSpam* > *Action*. Hacer clic en New.
2. Seleccionar el dominio en el que será de aplicación el perfil y un nombre identificativo.
3. Dentro del *AntiSpam Action Profile*, seleccionar los parámetros deseados, entre los cuales se encuentran:

- *Tag subject*: insertar una etiqueta predefinida en el asunto del mensaje.
- *Insert header:* insertar cabeceras personalizadas en el mensaje.
- *Insert disclaimer:* insertar una advertencia.
- *Deliver to alternate host:* entregar el mensaje original o modificado a un MTA alternativo.
- *Deliver to original host:* entregar el mensaje a la MTA original. Uno de los objetivos de esta redirección al host original podría ser, por ejemplo, dejar el mensaje original en cuarentena, con el objetivo de mandar al destinatario posteriormente el correo original saneado.
- *BCC:* agregar un destinatario específico en copia oculta.

- *Archive:* almacenar el mensaje en un archivo.
- *Notify:* notificar al remitente, destinatario u otra persona. El contenido de las notificaciones se puede personalizar (opción *New...*).
- Finalmente, con el correo se pueden realizar distintas acciones (*final action*):

  a) *Reject:* rechazar con el código SMTP 550. El mensaje de error se puede personalizar. De este modo, el servidor no tratará de reenviar el mensaje con la cadencia que tenga definida y el consumo de recursos asociado.

  b) *Discard:* aceptar y descartar el correo electrónico sin entregar.

  c) *Personal Quarantine:* mover el correo electrónico a la cuarentena personal para que el destinatario lo administre. Existen diferentes opciones. El administrador puede notificar al destinatario que un correo ha sido enviado a cuarentena mediante un informe. los vínculos incrustados en ese informe permiten al destinatario administrar los mensajes en cuarentena. El administrador también puede proporcionar acceso por correo web a la cuarentena personal del usuario.

  d) *System Quarantine:* Mover el correo electrónico a la cuarentena del sistema controlada por el administrador. El administrador puede crear varias cuarentenas de sistema diferentes.

  e) *Rewrite recipient address*: Reescribir la dirección de correo electrónico del destinatario y enviar el mensaje a la nueva.

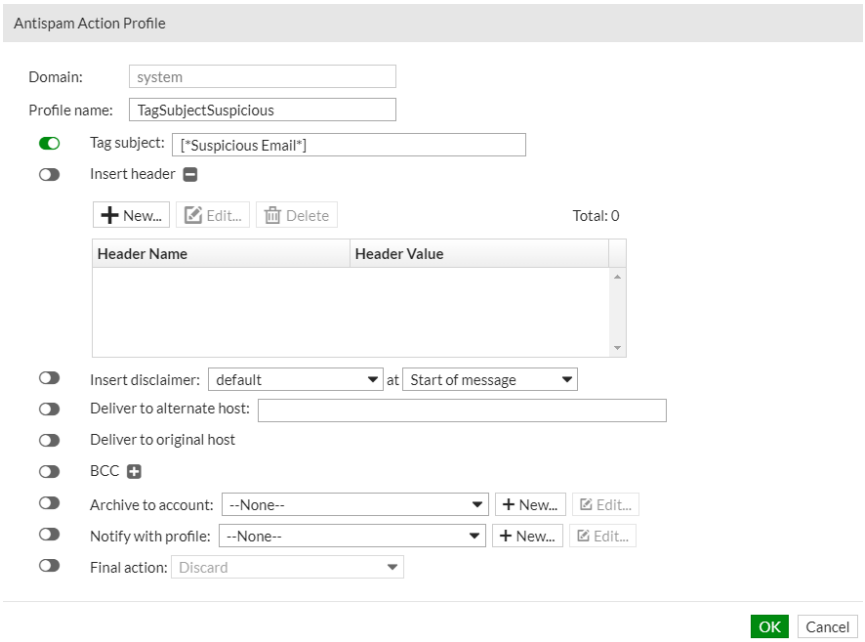


Figura 15. Acciones perfil anti-spam

7.3 BUSINESS EMAIL COMPROMISE (BEC)

220. Un método común utilizado por los atacantes es la suplantación de usuarios internos. Los correos electrónicos son falsificados, fingiendo ser de un usuario VIP o sensible interno para engañar a su destinatario con el fin de que divulgue información.

221. Esta funcionalidad detecta el uso de nombres de usuario internos que se originan en correos electrónicos desde fuera de la organización. Las asignaciones de direcciones válidas de los usuarios válidos se pueden identificar de varias maneras:

- Carga manual.
- Autodescubrimiento dinámico.

222. Al detectar estos correos, FortiMail puede notificar al destinatario para evitar este tipo de ataques de ingeniería social.

223. Para configurar esta funcionalidad, se debe crear un perfil BEC y asignarlo a la política deseada. Para ello:

- Ir a *Profile* > *AntiSpam* > *Impersionation*. Hacer clic en *New*.
- Configurar las opciones deseadas y hacer clic en *OK*.
- Asignar el perfil a la política deseada.

7.4 URI CLICK PROTECTION

224. Para evitar las protecciones sobre URIs, un atacante puede retrasar la activación de un sitio web malintencionado, o incluso, desde la entrega de un correo hasta el acceso a su enlace el sitio puede comprometerse. Por ejemplo, en caso de que un atacante envíe un correo electrónico que contenga una dirección URI segura, FortiMail y FortiSandbox escanean un correo electrónico el sitio web está limpio, sin embargo, después de un breve periodo de tiempo el atacante puede modificar la URI a una dirección maliciosa y esperar a que el usuario haga *click*.

225. *FortiMail Click Protection* reescribe los identificadores URI, todos u opcionalmente basados en categoría, de modo que cuando se hace clic en ellos, el usuario se redirige a FortiMail, donde el identificador URI se vuelve a analizar en el momento del clic mediante Filtrado de contenido web y FortiSandbox. Después de hacer clic, el usuario se redirigiría al URI original o se enviará una página de bloqueo en función del resultado del análisis.

226. La configuración de la protección sobre URIs se puede realizar desde *System* > *FortiGuard* > *URI Protection.*

7.5 IP BLACKLIST PROTECTION

227. Como proveedor de servicio de correo, se debe asegurar que la IP Pública no entre en listas negras impidiendo así el envío legítimo de mails. Muchas veces, ya sea a

propósito o de manera accidental (por una infección, por ejemplo), los usuarios enviarán spam pudiendo hacer que nuestra IP se comprometa afectando al servicio.

228. Para ello, incorpora esta característica que aplicará protección anti-spam también al tráfico saliente. Se proporcionan dos (2) opciones:

- **Inspección transparente:** el tráfico SMTP se enruta mediante *"policy based routing"* (gracias a routers o *firewalls*) o directamente el camino de estos paquetes tienen que atravesar forzosamente el FortiMail.

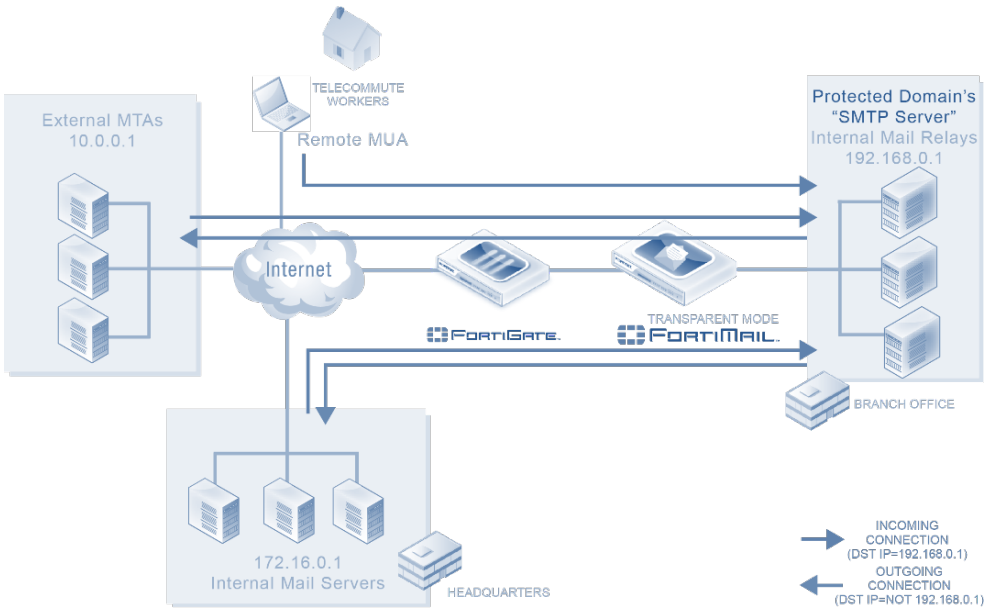


Figura 16. Ejemplo despliegue FortiMail en modo transparente

- **Proxy explícito:** Se configura el servidor de correo para que reenvíe también el correo saliente a FortiMail para su análisis y filtrado.

7.6 RECOLECCIÓN DE DIRECTORIOS Y PREVENCIÓN DE DOS

229. Gracias a la reputación del remitente, FortiMail es capaz de observar el comportamiento histórico del remitente en lugar de tratar cada mensaje por separado. Aunque la técnica de reputación del remitente en local se desarrolló originalmente para el escaneo de spam saliente y la prevención de listas negras, también es aplicable a la transmisión entrante. Usándolo de esta manera se puede obtener una reacción más rápida a nuevas campañas de spam y protección contra ataques de recolección de directorios (DHA).

230. Lo anterior combinado con la limitación de la velocidad de conexión por IP, mensaje, comando HELO, envío de rechazos (*reject*) y destinatarios permite defenderse contra ataques DoS.

231. En resumen, las mismas técnicas de seguridad aplicadas a los remitentes, se pueden aplicar a los usuarios dentro de nuestra organización, consiguiendo así prevenir

cualquier envío no autorizado, ya sea de manera consciente o de un cliente comprometido sin que él lo haya advertido.

7.7 CONTENT FILTERING

232. En muchos entornos la detección de información sensible que sale de la organización es una parte importante en la política de seguridad.

233. FortiMail es capaz de detectar y filtrar archivos adjuntos por nombre, tipo MIME y contenido. El análisis de diccionario permite un filtrado sencillo basado en palabras clave, expresiones regulares y sus combinaciones. Tanto el contenido del mensaje como los archivos adjuntos de tipo PDF y MS Office se pueden analizar con el diccionario. Como resultado, los mensajes pueden ser puestos en cuarentena, cifrados, archivados, bloqueados, etiquetados, reescritos o incluso enviados a un sistema externo para su procesamiento. Unido a esto, el motor de análisis de contenido multimedia permitirá también regular el contenido legítimo que circula vía correo electrónico en nuestra organización.

234. Para más información, consultar el apartado *"Configuring content profiles and content action profiles*" (página 429) de la Guía de Administración de FortiMail [REF1].

7.7.1 PERFILES DE CONTENIDO Y DICCIONARIO

235. El perfil de contenido está diseñado para proteger el envío de información confidencial por correo electrónico. El perfil de contenido busca información específica en los mensajes procesados. Los nombres de archivo, las extensiones de archivo y los tipos MIME se utilizan para identificar el contenido. También se puede manejar el intercambio de datos sensibles como pueden ser datos de tarjetas de crédito o información personal basándose en patrones incluidos con la solución o creando expresiones regulares ("*wildcards*") propias.

7.7.2 ARCHIVOS COMPRIMIDOS

236. Los archivos comprimidos con extensión *.zip, *.rar, *.gzip o similares se pueden descomprimir para su inspección. La compresión recursiva también es compatible con hasta 12 niveles de compresión. También se aplica la protección contra "*zip bombs",* limitando el tamaño máximo del archivo descomprimido.

7.7.3 CONTENIDO PROTEGIDO POR CONTRASEÑA

237. Los archivos protegidos por contraseña se pueden tratar de descifrar para su análisis y ejecutar una acción concreta en caso de no ser posible.

238. Para conseguir este objetivo y ser capaces de evaluar contenido cifrado, existen varias aproximaciones que pueden ser combinadas. Una de ellas será tratar de acceder al contenido probando con un número máximo (5 por defecto y configurable) de palabras encontradas dentro del cuerpo del email. Otra

aproximación sería utilizar los diccionarios incluidos en el dispositivo y, por último, también se puede activar la opción de probar el descifrado con un listado propio de palabras clave, que generalmente será un listado de contraseñas comunes o términos relacionados con el negocio.

239. A continuación, se describe el procedimiento de configuración de opciones de descifrado de contraseñas:

1. Ir a *Profile* > *Content.*
2. Hacer click en *New* para crear un nuevo perfil, o seleccionar un perfil existente para modificarlo.
3. Expandir la opción *File Password Decryption Options*.
4. Especificar los tipos de contraseña a emplear. Se ofrecen varias opciones:
   - Palabras en el contenido del email.
   - Listado predefinido de contraseñas.
   - Listado de contraseñas definido por el usuario.

240. Este procedimiento se describe en detalle en el apartado "*Configuring password decryption options*" (página 435) de la Guía de Administración de FortiMail [REF1].

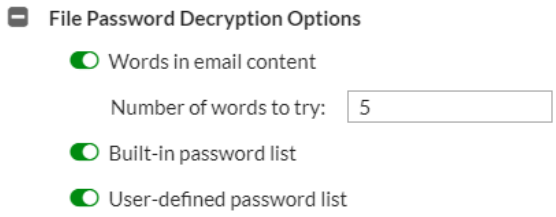


Figura 17. Descifrado de ficheros

7.7.4 DOCUMENTOS INCRUSTADOS

241. Gracias a la funcionalidad de *Content Disarm and Reconstruction*, en el caso de encontrar un fichero adjunto/incrustado dentro del email será posible tomar distintas acciones. Entre ellas, se podrá neutralizar una macro dentro de un documento de MS Office o desactivar el código embebido en un documento PDF, mientras se entrega el resto del contenido a su destinatario.

242. De esta manera se eliminará cualquier contenido potencialmente peligroso, que por ejemplo se haya enviado de manera involuntaria por un remitente infectado, deteniendo su propagación.

243. El contenido original, sin "higienizar", está disponible dentro del sistema de cuarentena y se podrá recuperar o liberar sin modificaciones al receptor inicial.

244. Para más información, consultar *Content Disarm and Reconstruction Recipe* [REF14].

7.7.5 DYNAMIC DLP

245. El motor de DLP permitirá la prevención o exfiltración de datos sensibles de la organización. Se definirán diferentes patrones, los cuales, en caso de encajar, permitirán aplicar distintas acciones a ejecutar sobre el correo en cuestión. Además de las expresiones regulares que se definan, FortiMail cuenta con patrones preconfigurados como datos de tarjetas y números asociados a datos sanitarios, que podrán ser utilizados simplemente seleccionándolos en un menú desplegable. Más información en "*Configuring DLP profiles*" (página 553) de la Guía de Administración de FortiMail [REF1]

8. FASE DE OPERACIÓN

246. Una vez el producto está configurado de forma segura y se encuentra en modo de funcionamiento normal, se deben llevar a cabo las siguientes tareas de mantenimiento:

- **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.
- **Comprobaciones periódicas de la correcta operación de los algoritmos y funciones criptográficas**, a través de la ejecución de los correspondientes auto-chequeos.
- **Actualizaciones periódicas del *software*** de los equipos, para garantizar que están al día, tanto en las capacidades de protección, como en funcionalidades avanzadas.
- **Realización de "*backups*"** automáticos de forma periódica y, a poder ser, de forma centralizada.
- **Mantenimiento de los registros de auditoria**. Estos registros estarán protegidos de borrados y modificaciones no autorizadas, y solamente el "*super administrador*" podrá acceder a ellos. La información de auditoria se guardará en las condiciones y por el periodo establecido en la normativa de seguridad.
- **Auditar**, al menos, los eventos especificados en la normativa de referencia y aquellos otros extraídos del análisis de riesgos.
- **Hacer crecer la base de datos de muestras de análisis bayesiano** (ver el apartado 7.1.13 BAYESIAN SCAN) para optimizar la detección basándose en la experiencia real del servicio.
- **Concienciar a los usuarios** sobre el uso del correo y las amenazas más extendidas del correo electrónico.
- **Análisis periódico de los *reports*** (informes) y cuadros de mando incorporados con la solución. Una anomalía en el comportamiento del servicio de correo puede ser detectada fácilmente con, por ejemplo, el panel de número de correos procesados. Una gran discrepancia entre dos medidas implica un comportamiento extraño.
- **Gestión periódica de la cuarentena**, tanto global como de los usuarios.
- **Verificar y monitorizar** la reputación pública de las IPs definidas para el servicio.

9. CHECKLIST

247. La siguiente checklist contiene todas las recomendaciones sobre la configuración relativas al FortiMail:

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto	☐	☐	
Instalación en un entorno seguro	☐	☐	
Registro del producto	☐	☐	
CONFIGURACIÓN			
CONFIGURACIÓN DEL MODO DE OPERACIÓN SEGURO			
Activación del comando que establece el modo de operación seguro	☐	☐	
Deshabilitado de los protocolos SSH, Telnet y HTTP	☐	☐	
AUTENTICACIÓN REMOTA			
Habilitación de HTTPS	☐	☐	
Configuración de TLS	☐	☐	
CONFIGURACIÓN DE AUTENTICACIÓN			
Establecimiento contraseñas / Configuración de clave pública	☐	☐	
Establecimiento de política de contraseñas	☐	☐	
Configuración de servidores externos de autenticación	☐	☐	
Configuración de reglas de autenticación de conexiones SMTP			
CONFIGURACIÓN DE LOS PARÁMETROS DE SESIÓN			
Configuración de tiempos de sesión e intentos de login fallidos	☐	☐	
Configuración del Login Banner	☐	☐	
CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS			
Deshabilitado de interfaces	☐	☐	

ACCIONES	SÍ	NO	OBSERVACIONES
CERTIFICADOS			
Instalación de certificados de servidor	☐	☐	
Instalación de certificados de CA	☐	☐	
Configuración de CRLs / OCSP	☐	☐	
PERFILES			
Configuración de cuentas de administración / webmail	☐	☐	
Configuración de perfiles TLS	☐	☐	
Configuración de perfiles de cifrado IBE	☐	☐	
Configuración de perfiles de cifrado S/MIME	☐	☐	
CONFIGURACIÓN DE LA SINCRONIZACIÓN HORARIA			
Configuración de fecha y hora local	☐	☐	
CONFIGURACIÓN DE ACTUALIZACIONES			
Configuración de actualizaciones automáticas	☐	☐	
CONFIGURACIÓN DE ALTA DISPONIBILIDAD			
Establecimiento de configuración A-A / A-P	☐	☐	
CONFIGURACIÓN DE AUDITORÍA			
Configuración de eventos en el almacenamiento local	☐	☐	
Configuración del envío de eventos al servidor remoto (syslog / FortiAnalyzer / SIEM)	☐	☐	
COPIAS DE SEGURIDAD			
Realización del backup de la configuración de los equipos	☐	☐	
CONFIGURACIÓN ANTI-SPAM			
Establecimiento de dominios	☐	☐	
Configuración de perfiles	☐	☐	
Establecimiento de políticas de control de acceso	☐	☐	

10. REFERENCIAS

REF1 Guía de Administración de FortiMail 6.2 *Administration Guide*

REF2 Guía de comandos CLI FortiMail 6.2 *CLI Reference*

REF3 Log Reference *Log Reference*

REF4 Evitar Blacklisting

How Does an ISP Avoid Blacklisting

REF5 Solución IBE para cifrado

Encrypting Confidential Emails in FortiMail

REF6 *Logging* remoto en FortiAnalyzer

Remote Logging in FortiMail Using FortiAnalyzer

REF7 Instalación segura de *Firmware*

How to Perform a Clean FortiMail Firmware Installation

REF8 Configuración A-A FortiMail

How to Set up a Config-Only HA in FortiMail

REF9 Configuración A-P FortiMail

How to Set up an Active Passive HA in FortiMail

REF10 *FortiMail en modo pasarela*

Deploying FortiMail Gateway Mode

REF12 *Fortinet Support Website Guide*

Fortinet Support Portal for Product Registration, Contact Registration, Ticket Management, and Account Management

REF13 Página web de soporte de Fortinet

Página de soporte de Fortinet

REF14 *Content Disarm and Reconstruction (CDR)*

Content disarm and reconstruction recipe

REF 15 *How to Install FortiMail Firmware Using the CLI*

https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/63a90f6c-9392-11e9-81a4-00505692583a/How_to_Install_FortiMail_Firmware_Using_the_CLI.pdf

11. ABREVIATURAS

API	*Application Programing interface – Interfaz de programación de aplicaciones.*
BCC	*Blind Carbon Copy – Copia de carbón oculta.*
CA	*Certification Authority – Autoridad de certificación.*
CLI	*Command Line Interface- Interfaz de línea de comandos*
CPD	*Centro de Procesamiento de Datos.*
CRL	*Certificate Revocation List – Lista de revocación de certificados*
DKIM	*DomainKeys Identified Mail – Correo identificado por DomainKeys.*
DLP	*Data Leak Prevention – Prevención de filtración de información.*
DMARC	*Domain-based Message Authentication, Reporting and Conformance - Autenticación de mensajes, informes y conformidad basada en dominios.*
DNS	*Domain Name System – Sistema de nombres de dominio.*
DNSBL	*DNS Blocked List – Lista negra basada en DNS.*
ENS	*Esquema Nacional de Seguridad.*
GUI	*Graphical User Interface – Interfaz gráfica de usuario.*
HA	*High Availability – Alta disponibilidad.*
HTTP	*Hypertext Transfer Protocol – Protocolo de transferencia de hipertexto.*
IBE	*Identity Based Encryption – Cifrado basado en identidad.*
IMAP	*Internet Message Access Protocol – Protocolo de acceso a mensajes de internet.*
LDAP	*Lightweight Directory Access Protocol – Protocolo ligero de acceso directo.*
MIME	*Multipurpose Internet Mail Extensions – Extensiones multipropósito de correo de internet.*
MTA	*Message Transfer Agent – Agente de transmisión de mensajes.*
NAS	*Network Attached Storage – Almacenamiento conectado en red.*
OCSP	*Online Certificate Status Protocol – Protocolo de comprobación del estado de certificado en línea.*

PKI	*Public Key Infrastructure – Infraestructura de clave pública.*
POP3	*Post Office Protocol – Protocolo de oficina de correo.*
RADIUS	*Remote Authentication Dial-In User Service – Servicio de usuario de autenticación remota.*
RBL	*Real-Time Blackhole List – Lista de agujeros negros en tiempo real.*
SIEM	*Security Information and Event Management – Gestión de información y eventos de seguridad.*
SMTP	*Simple Mail Transfer Protocol - Protocolo para transferencia simple de correo.*
SPF	*Sender Policy Framework – Convenio de Remitentes.*
SPF	*Sender Policy Framework – Marco de política de remitente.*
SSH	*Secure Shell – Intérprete de comandos seguro.*
SURBL	*Spam URI RBL.*
TLS	*Transport Layer Security – Seguridad de la capa de transporte*
URI	*Uniform Resource Identifier – Identificador de recursos uniforme.*