

Fortinet FortiMail sobre *appliance* FortiMail-2000A

Se identifica, examina, analiza, valora y evalúa FortiMail, una herramienta de seguridad de red de naturaleza hardware-software, robusta, de gran flexibilidad, del tipo sistema especializado multinivel de seguridad para el servicio de correo-e sobre el *appliance* FortiMail-2000A. De elevado rendimiento y con características de tolerancia a fallos, alta disponibilidad y redundancia, la solución de Fortinet protege contra amenazas y ataques, incluye capacidades de archivo de correo y registro de tráfico entrante y saliente de correo, soporta funcionalidades de QoS, virtualización y encaminamiento de correo-e bi-direccional, se gestiona de forma centralizada desde un PC de administración dotado de interfaz GUI y soporta CLI. Asimismo, permite desplegar políticas de seguridad basadas en el receptor y en la dirección IP, e integra funcionalidades de gestión de *logs* y generación de informes a medida. Respecto a su despliegue, posibilita llevarlo a cabo en tres modalidades (transparente, servidor y pasarela) y no presenta restricciones en cuanto al número de usuarios y de buzones.

IDENTIFICACIÓN DE LA HERRAMIENTA

La herramienta de seguridad hardware-software *FortiMail* sobre *appliance FortiMail-2000A* de la compañía Fortinet, Inc. puede catalogarse como un sistema especializado de seguridad que permite proteger, con filosofía multinivel, el servicio de correo electrónico entrante/saliente contra amenazas y ataques como DoS (*Denial of Service*)/DDoS, DHA (*Directory Harvest Attacks*), RBL (*Real-Time Black List*), *spam-phishing* y contenido malicioso (virus, gusanos, *spyware*, *malware*, *zombies*, *bots*, etc.). Asimismo, posibilita aplicar políticas de seguridad a los contenidos de correo de la compañía y permite archivar contenidos de correo en buen estado.

FortiMail
FORTINET.

FortiMail se actualiza de forma continua; por ejemplo, sus motores de exploración basados en firmas, de tipo heurístico, etc. así como sus firmas de amenazas a través de los Servicios de suscripción de *FortiGuard*, que son apoyados por un prestigioso equipo de investigación de amenazas 24x7 a nivel mundial.

CARACTERÍSTICAS MÁS RELEVANTES

Entre las características más relevantes identificadas en esta herramienta se pueden indicar: **1) Seguridad multinivel.** Integra un rico conjunto de funcionalidades de protección *antispam*, *antivirus*, *antispyware*, *anti-DoS/DDoS*, etc. Soporta un modelo de cuarentena para ficheros infectados. **2) Alto rendimiento.** Incorpora un motor especializado de tratamiento de mensajes de correo-e basado en estándares MTA (*Mail Transfer Agent*) que proporciona niveles elevados de rendimiento, aplicando encaminamiento inteligente y políticas de QoS. **3) Sin restricciones en cuanto al número de usuarios**

y número de buzones (o mailboxes). **4) Flexibilidad de despliegue.** Soporta tres modos de operación: modo pasarela, modo transparente y modo servidor. **5) Alta fiabilidad, tolerancia a fallos, disponibilidad y redundancia.** Soporta fuentes de alimentación eléctrica *hot swappable*, configuración de almacenamiento en disco duro tipo RAID, redundancia de ventiladores y posibilidad de operar con varias unidades hardware para implantar configuraciones de máxima tolerancia a fallos. **6) Archivo de correos local y remoto.** Incluye capacidades de visibilidad y auditoría en todos los aspectos de la utilización del correo-e para ayudar a aplicar las políticas de utilización. **7) Funcionalidades de gestión de logs y generación de informes.** Proporciona un registro de eventos del funcionamiento antivirus, *antispam*, etc., así mismo posibilita la generación de informes a medida en diversas modalidades, como la personalizada y la planificada. Permite, por ejemplo, conocer por qué razones un correo se consideró *spam*, de quién provenía, a quién iba dirigido, etc.

MODOS DE OPERACIÓN-DESPLIEGUE

La herramienta de Fortinet aquí evaluada se ha constatado que soporta tres modos de operación-despliegue:

1) Modo pasarela.

Proporciona funcionalidades antivirus, *antispam*, filtrado de contenidos, encaminamiento y archivo de correo electrónico, monitorización y servicios de generación de informes a la infraestructura de correo actual con muy pocos cambios en la red. Todos los interfaces del *appliance* hardware se encuentran en diferentes subredes IP. En este modo, el *appliance* actúa como un servidor de retransmisión de correo, no proporciona buzones locales pero proporciona una interfaz de usuario Web para gestionar filtros de *spam* (listas negras/grises), gestión de base de datos Bayesiana por usuario, etc. En este modo se proporcionan las siguientes funcionalidades:

- i) Actúa como una pasarela delante de los servidores de correo existentes.
- ii) Soporta exploración de correo entrante y saliente.
- iii) Proporciona encaminamiento de correo basado en dirección IP y en el destinatario.
- iv) Puede actuar como un sistema de retransmisión saliente para incrementar la seguridad.
- v) Proporciona administración por niveles.
- vi) Soporta grupos de usuarios de dominios, alias de correo electrónico y re-escritura de direcciones de correo.
- vii) Soporta configuraciones de *fail-over* para alta disponibilidad y tolerancia a fallos.
- viii) Requiere el cambio del

El *appliance* FortiMail 2000A de Fortinet es una herramienta de seguridad de red flexible, de elevado rendimiento y características de tolerancia a fallos y alta disponibilidad, catalogada como sistema especializado multinivel-multifuncional de protección para el servicio de correo-e entrante y saliente. Incorpora una gestión centralizada rica en funcionalidades, soporta tres modos de despliegue y gestión de *logs* y aporta una generación de informes muy cuidada, además de poder almacenar correo y operar con mecanismo de cuarentena.

registro MX DNS que redirija los correos al *appliance* FortiMail-2000A antes de que alcancen el servidor de correo corporativo. Puede aceptar, retransmitir, rechazar o descartar correo en base a la dirección de correo, dirección IP o dominio. ix) Explora mensajes de correo SMTP en busca de virus, *spam* y adjuntos/contenido prohibido. x) Proporciona acciones múltiples para gestionar virus, correo *spam*, y contenido prohibido, incluyendo cuarentena o etiquetas, eliminando adjuntos, sustituyendo el cuerpo del mensaje, etc. xi) Soporta archivo de mensajes entrantes y salientes en base a políticas de usuario. xii) Proporciona monitorización, registro y generación de informes. xiii) Proporciona acceso Webmail y resumen diario de correos para procesar el correo en cuarentena. xiv) Soporta dominios y redes de correo múltiples. xv) Soporta listas negras/blancas del sistema, listas negras/blancas de sesión y listas negras/blancas personales.

2) Modo transparente.

Se coloca delante del servidor de correo existente y presenta una integración imperceptible en el entorno de red donde se ubica. Permite colocar el *appliance* en la red sin realizar ningún cambio de dirección IP. Cuando se opera en modo transparente, todas las interfaces de la unidad hardware se encuentran en la misma subred IP y el *appliance* actúa como un puente. Todas las características del modo pasarela se encuentran disponibles cuando opera en modo transparente pero no se necesitan cambios en los registros MX DNS.

3) Modo servidor.

Se coloca detrás de la unidad de retransmisión de correo corporativo. Proporciona una funcionalidad completa de servidor de correo además de funcionalidades antivirus, *antispam* y de archivo de correos-e. Proporciona todas las funcionalidades del modo pasarela más las siguientes: i) Proporciona servicios de correo Webmail, IMAP, SMTP y POP3. ii) Proporciona acceso a clientes Webmail con SSL. iii) Soporta políticas de cuota de disco para cuentas de usuario. iv) Proporciona listas de alias, grupos y usuarios. v) Coloca los correos *spam* en la carpeta a granel del receptor.

CONFIGURACIÓN Y GESTIÓN DEL APPLIANCE

Una vez instalada la unidad hardware (o *appliance*) se puede configurar y gestionarla. Se ha constatado que existen dos métodos fundamentales de conectar y configurar el *appliance*, bien utilizando: 1) **Gestor basado en web.** Se pueden identificar dos niveles de gestión: i) Para los usuarios administradores nuevos posibilita un modo de gestión básico. (ii) Cuando los administradores obtienen suficiente experiencia posibilita un modo de gestión avanzado que permite todas las opciones de configuración. Es posible configurar, gestionar y monitorizar el estado de la unidad hardware utilizando *http* o *https* (mejor opción) a través de un computador que opere en red con el navegador Internet Explorer 6.0. Los cambios de configuración son efectivos de forma inmediata sin resetear la unidad hardware o interrumpir el servicio. 2) **Una interfaz de línea de comandos o CLI.** Se puede acceder a la interfaz CLI conectando al puerto serie de un PC de gestión al conector DB9 de consola serie situado en el *appliance*. Se puede utilizar una conexión Telnet o mejor SSH para conectarse al CLI desde cualquier red a la que esté conectado el *appliance*, incluido Internet. La CLI soporta la misma configuración y funcionalidades de monitorización que el gestor basado en Web, además se puede utilizar la CLI para opciones de configuración avanzadas que no son disponibles desde el gestor basado en web básico.

TIPOS DE PERFILES

La herramienta aquí valorada incluye como perfiles por defecto el *antispam*, antivirus y de contenidos. Se ha constatado que soporta los siguientes tipos de perfiles:

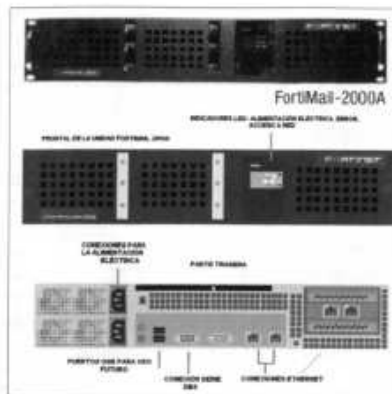


Fig. 1.- Aspecto delantero y trasero de la unidad hardware FortiMail-2000A.

1) Perfil antispam.

Se utiliza para definir los métodos *antispam* que se permiten, así como especificar los parámetros de configuración y establecer las acciones a tomar cuando se identifique un mensaje de *spam*. Pueden definirse múltiples perfiles *antispam* entrantes y salientes.

El perfil *antispam* puede utilizarse tanto en las políticas basadas en el receptor como las basadas en dirección IP.

Posibles acciones que pueden tomarse son: i) Etiquetar el correo



Fig. 2.- Configuración RAID general.

en la línea del *subject* (la etiqueta se puede personalizar). ii) Etiquetar el correo con una cabecera (la etiqueta se puede personalizar a medida). iii) Rechazarlo avisando (el mensaje de rechazo se puede personalizar). iv) Descartarlo sin avisar. v) Meterlo en zona de cuarentena. vi) Permitir a los usuarios que automáticamente actualicen la lista blanca personal de correos enviados. vii) Reenviar a una dirección de correo. La etiqueta y las acciones se pueden combinar con opciones de rechazo, descartar, cuarentena y listas blancas aunque las opciones de rechazo, descartar y cuarentena son mutuamente excluyentes. Los perfiles *antispam*

EQUIPOS UTILIZADOS EN LA EVALUACIÓN

- Equipamiento para estación de gestión, puestos de trabajo de usuarios, servidores y *appliances* virtuales con Windows 2003/2000/XP, PCs con procesador Intel Dual Core 2 GHz., con 2Gb de memoria, disco duro de 160 Gb, unidad DVD/CD-ROM, tarjeta gráfica WXGA, tarjeta NIC de red 10/100/1000Base T compatible NE2000/NDIS. Navegador Internet Explorer 6.0. Servidores LDAP, NAS, Web, Radius, SMTP, POP3, IMAP4.
- Nueve redes locales, Ethernet 10/100/1000 BaseT con IEEE 802.2-LLC, como soporte físico de las comunicaciones con Protocolo de Control de Acceso al Medio o MAC CSMA/CD. Acceso a Internet.
- Hubs/Switches de 16 puertos Ethernet 10/100/1000. Módems analógicos para RTB/RTC V.90/ITU-TSS (a 56 Kbps) y tarjetas digitales RDSI-BE 2B+D/Acceso Básico-BRA como acceso conmutado al exterior y conexiones ADSL/cable modem. Acceso GSM/GPRS/UMTS. Ocho routers. Cuatro puntos de acceso Wi-Fi, IEEE 802.11g/b/a. Seis impresoras. Un *appliance* FortiMail-2000A.
- Analizador de protocolos para monitorizar las comunicaciones intercambiadas en todos los niveles de la arquitectura.
- Módulos de valoración de mecanismos criptográficos de cifrados, autenticación. Módulo de valoración de criptoanálisis con cálculo no intensivo.
- Módulo de pruebas para medidas de seguridad y rendimiento con diferentes cargas de trabajo y número de usuarios.
- Generadores de tráfico.
- Baterías de ataques y amenazas (*malware*, *spam*, *phishing*, DoS/DDoS, gusanos, *bots*, zombis, virus, etc.) bajo control gestionable de cargas de tráfico.
- Mecanismos de valoración para pruebas "side-channel".

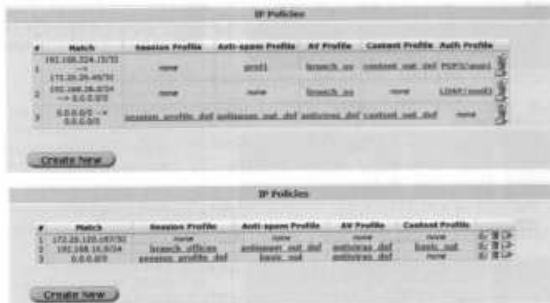


Fig. 3.- Especificación de una lista de política basada en IP en la modalidad pasarela y servidor con FortiMail v2.8.

salientes utilizan un subconjunto de las opciones de perfil antispam entrante. El administrador puede especificar un tamaño máximo de mensaje para explorar spam y permitir a los usuarios actualizar sus listas blancas personales del correo enviado. Soporta el saltarse la exploración antispam para usuarios autenticados.

2) Perfil antivirus.

Se pueden definir múltiples perfiles. Se utiliza para permitir o no la exploración antivirus. También permite ver la lista de firma de virus actual. Se puede utilizar tanto en la política basada en el receptor como la basada en la dirección IP. Se ha podido constatar que la herramienta aquí evaluada soporta diferentes acciones cuando un virus se detecta en base a una firma: (i) Reemplazar el cuerpo del virus. (ii) Rechazarlo. (iii) Descartarlo. Si se detecta en base a una exploración heurística: (i) Reemplazar adjuntos sospechosos. (ii) Rechazarlo. (iii) Descartarlo.

3) Perfil de autenticación y LDAP.

Se pueden definir múltiples perfiles de autenticación utilizando como método para ello LDAP, Radius, POP3, IMAP y SMTP. Se utiliza para definir los parámetros del servidor utilizado en ese perfil como dirección del servidor, puerto, etc. Se puede utilizar tanto en la política basada en el receptor como la basada en la dirección IP.

4) Perfil de contenidos.

Permite manipular filtros de contenidos y adjuntos. Define las reglas de filtrado de tipo de fichero y adjunto, el perfil de diccionario utiliza el monitor de contenido y las acciones que toma cuando un correo incluye un adjunto que incumple las reglas. Se puede utilizar tanto en la política basada en el receptor como la basada en dirección IP. El filtrado de adjuntos se utiliza para bloquear adjuntos en base a la extensión del fichero. Cualquier extensión de fichero puede añadirse a la lista, pero este filtrado de adjuntos no comprueba si el tipo de fichero es del tipo que debe bloquearse, por ejemplo, si se bloquean ficheros .doc, este filtro de adjuntos bloqueará todos los ficheros con extensión .doc sin inspeccionar el fichero. Si un fichero .doc se renombra y se envía como .txt, este filtro de adjuntos no detectará el fraude.

También soporta el filtrado de tipo de fichero que se utiliza para bloquear adjuntos en base al tipo de fichero, en este caso se inspecciona el fichero para saber si está o no permitido. La herramienta bajo evaluación puede filtrar los siguientes tipos de ficheros: video (.mp3, .avi, etc.), audio, imagen (.jpg, .bmp, .tiff, etc.), aplicación-ejecutables (.exe, etc.), aplicación-documentos (.doc, etc.), aplicación-archivos y otros tipos de aplicación. Al detectarse un adjunto no autorizado en base al tipo de fichero, permite tomar las siguientes

acciones: tratarlo como spam, rechazarlo, descartarlo, reemplazarlo (con un mensaje de sustitución personalizado), meterlo en cuarentena, reenviarlo a una dirección de correo electrónico. Las acciones del perfil de contenido son mutuamente excluyentes. El monitor de contenido puede utilizarse para aplicar exploraciones de diccionario al cuerpo del mensaje y a los adjuntos de acuerdo a un perfil de diccionario.

5) Perfil Misc.

Sólo opera en el modo servidor. Incluye las siguientes configuraciones: cuota de disco (por usuario), estado de cuenta de usuario (permitir/inhabilitar), acceso Webmail (permitir/inhabilitar).

6) Perfil de sesión.

Proporciona protección de correo a nivel de sesión y sólo se puede utilizar en políticas basadas en dirección IP. Son posibles múltiples opciones de configuración: i) Opciones-configuración de conexión: ocultar la herramienta del servidor de correo, restringir conexiones del cliente, bloquear conexiones del cliente a servidores SMTP de listas negras, etc. ii) Opciones-configuración sobre reputación del emisor: restricciones del número de correos por hora, rechazo del cliente, etc. iii) Opciones-configuración sobre sesión: permitir SMTP pipelining (sólo en modo transparente), rechazar comandos EHLO/HELO con caracteres no válidos, realizar comprobaciones sin tácticas estrictas, etc. iv) Opciones-configuración sobre sesiones no autenticadas: comprobar dominio del emisor y del receptor, rechazar dominios vacíos, rechazar conexión si coinciden los dominios del receptor y de HELO pero el dominio del emisor es diferentes. v) Opciones-configuración sobre limitaciones del SMTP: restringir el número de EHLO/HELO por sesión, restringir número de correos por sesión, restringir número de receptores por correo, etc. vi) Opciones-configuración sobre gestión de errores: tirar abajo la conexión después de un número específico de errores, establecer el número de errores que a un cliente se le permite, etc. vii) Opciones-configuración referentes a listas: permitir al emisor comprobar en listas blancas/negras, permitir o inhabilitar receptores en base a una lista.

7) Perfil de diccionario.

Se utiliza para definir palabras y patrones que la herramienta puede emplear en un perfil antispam o de contenido; por ejemplo, un perfil de diccionario se puede utilizar para detectar contenido sensible (por ejemplo, datos médicos), prohibido o para detectar spam. Un perfil de diccionario contiene definiciones y grupos, los diccionarios son específicos de dominio y la definición de diccionario contiene categorías y lenguajes que son identificadores que permiten crear perfiles de diccionario simples o complejos.

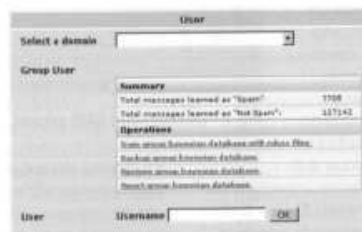


Fig. 4.- Opciones de base de datos bayesiana con FortiMail v2.8.



Fig. 5.- Configuración de la interfaz en modo pasarela.

DESPLIEGUE DE POLÍTICAS DE SEGURIDAD

Las políticas pueden dividirse en dos grandes categorías: las basadas en el receptor y las basadas en la dirección IP.

1) Políticas basadas en el receptor.

A su vez pueden identificarse dos subcategorías: i) Políticas de correo entrante. Se definen por dominio y se pueden dividir en políticas específicas por usuario. El administrador especifica una lista de usuarios y los perfiles de autenticación, antispam y antivirus que aplica a cada usuario en ese dominio. El usuario puede ser una dirección de correo completa o se pueden utilizar caracteres comodín para especificar un colectivo. La verificación del receptor la soporta el servidor SMTP o LDAP. Si un servidor LDAP se usa para la verificación del receptor es posible aplicar los perfiles antispam y antivirus por usuario utilizando una búsqueda LDAP en vez de especificar manualmente los usuarios individuales en la política. Se ha

constatado que es posible restringir el uso de diferentes identidades del emisor como parte de definiciones de la política de usuario. Si se permite la autenticación SMTP, el administrador puede elegir permitir o no diferentes identidades emisoras. Si esta configuración se activa con la opción *no permitir*, significa que un usuario de una dirección debe coincidir con su dirección de cuenta de correo-e actual en el servidor utilizado para la autenticación SMTP. **ii) Políticas de correo saliente.** Las políticas de correo saliente se utilizan para realizar exploraciones antivirus y antispam en el correo enviado desde usuarios internos a destinos de Internet. Se crean sólo para cada usuario. Soporta caracteres comodín, por ejemplo *@xxx.net.

2) Políticas basadas en la dirección IP.

Se definen en base a las direcciones IP del servidor y del cliente en modo transparente. En los modos servidor y pasarela sólo se especifica la dirección IP del cliente. No existe el concepto de políticas basadas en IP para correo entrante y saliente ya que las direcciones IP del cliente y del servidor definen la dirección del flujo de tráfico de correo. Las políticas basadas en dirección IP soportan perfiles antispam, antivirus, de contenidos, de sesión y de autenticación. Las opciones incluyen rechazo de conexiones que concuerdan con el perfil y saltarse la política basada en el receptor si la conexión concuerda con la política basada en dirección IP.

Cabe destacar que la herramienta bajo evaluación de Fortinet soporta exploración antivirus y antispam por usuario utilizando atributos LDAP por política. El servidor LDAP establece la configuración de política que permite especificar un atributo antivirus y antispam. Se puede utilizar un atributo existente para crear uno nuevo para cada configuración. También soporta encaminamiento de correo basado en LDAP sobre una base de dominio.

FUNCIONALIDAD DE ARCHIVO DE CORREOS ELECTRÓNICOS

La herramienta aquí evaluada incluye una funcionalidad útil de archivo de correos electrónicos que puede utilizarse para soportar requisitos de regulación de archivo de correos y puede realizarse en el disco local de FortiMail-2000A o descargándolos en un servidor remoto vía FTP o SFTP (mejor opción). Los administradores pueden ver o descargarse localmente el correo archivado utilizando un cliente estándar de correo electrónico sobre POP3 o IMAP4. El correo archivado localmente puede verse (pero no descargarse) usando la interfaz GUI de administración.

Las políticas de archivo permiten seleccionar en base a parámetros: dirección destino, dirección del receptor, palabras clave del cuerpo, nombre del fichero adjunto, etc. Pueden definirse varias políticas de archivo y se permiten

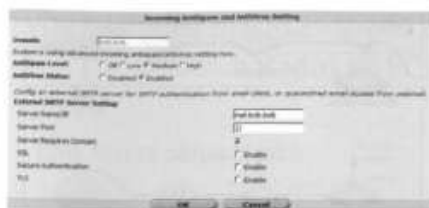


Fig. 6.- Configuración antivirus-antispam correo entrante con la herramienta FortiMail v2.8.

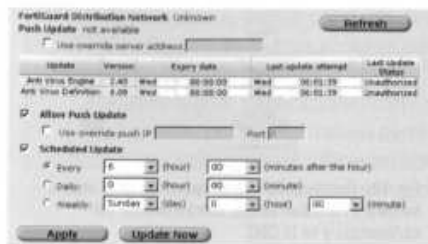


Fig. 7.- Actualización de FortiGuard de definición y motores anti-virus con FortiMail v2.8.

Name	Description	Priority
Replacement	Replacement message for mail virus	50
Virus message	Replacement message for selected email attachments	50
Content-based message	Replacement message for suspicious email attachments	50
Attachment filtering message	Replacement message for email containing banned attachments	50
Content filtering message	Replacement message for the link of email containing sensitive contents	50
Content filtering subject	Replacement message for the subject of email containing sensitive contents	50
Reject	Reject message for mail virus	50
Virus message	Reject message for email containing virus	50
Content-based message	Reject message for email containing suspicious contents	50
Attachment filtering message	Reject message for email containing banned attachments	50
Content filtering message	Reject message for email containing sensitive contents	50
Content filtering subject	Reject message for email containing sensitive contents	50
Spam report (HTML)	Message body for spam reports (HTML)	50
Spam report (Text)	Message body for spam reports (Text)	50
Spam Report Subject	Spam Subject line for Spam Report (Text)	50

Fig. 8.- Lista de mensajes personalizada con la herramienta de Fortinet.

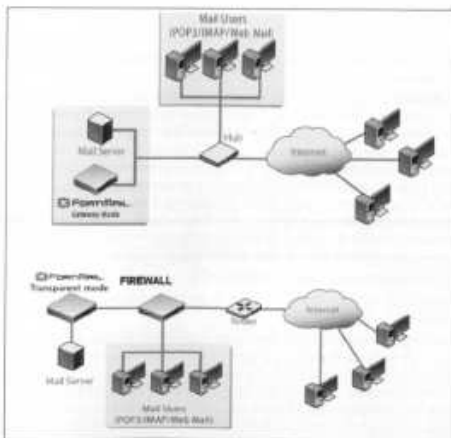


Fig. 9.- Despliegues en modos pasarela y transparente de la unidad hardware FortiMail-2000A.

múltiples listas de exclusión en base a patrones de dirección del emisor o del receptor. Las políticas de correo-e se encuentran separadas de las políticas entrantes y salientes. Las políticas de archivo de correos se aplican a todo el tráfico de correos que atraviesan el hardware FortiMail-2000A independientemente de la dirección. El producto aquí evaluado proporciona la capacidad para navegar sobre el correo archivado utilizando la interfaz GUI de administración. Se ha constatado que incluye la capacidad de reenviar correo archivado a una dirección de correo concreta.

HARDWARE DEL APPLIANCE FORTIMAIL-2000A

Una exploración física del hardware FortiMail 2000A, permite identificar los siguientes elementos más destacados:

- 1) En la parte delantera se sitúan:
 - i) Seis unidades discos duros extraíbles Western Digital de 250 GB (WD2500YS). La capacidad total del disco duro es de 1,5 TBytes (pudiendo llegar hasta 2,4 TB). La gestión de almacenamiento en disco incorpora la tecnología RAID (0, 1, 5, 10, 50) para integridad y tolerancia a fallos.
 - ii) Dos puertos USB.
 - iii) Cuatro leds indicadores: alimentación eléctrica, acceso al dispositivo de arranque, actividad en el puerto 1 y en el puerto 2.
 - iv) Tres botones incluido el de reset.
- 2) En la parte posterior se ubican:
 - (i) Dos fuentes de alimentación eléctrica extraíbles redundantes hot swappable. Opera con corriente alterna a 100-240 voltios a 50/60 Hz. con un consumo de unos 340 vatios.
 - (ii) Dos puertos PS/2.
 - (iii) Dos puertos USB.
 - (iv) Un puerto serie RS232 con conector DB9 a 9600 bps.
 - (v) Un puerto VGA.
 - (vi) Cuatro puertos Ethernet separados 10/100/1000 Mbps Base-T. Su peso aproximado es de 16 Kg. En la parte interna la unidad hardware FortiMail 2000A utiliza un sistema operativo extra-recortado a medida e incorpora una CPU con Dual Xeon 2,8 GHz., y memoria RAM es de 2GB.

GENERACIÓN DE INFORMES A MEDIDA

La herramienta aquí valorada descarga los ficheros de log al PC de administración utilizando el GUI de administrador, así mismo envía por correo ficheros de log a uno o más direcciones de correo especificadas por el administrador. Además, permite ejecutar informes por dominio y descargar informes en formato pdf.

Se ha constatado que incluye ocho diferentes categorías de informes. Los informes pueden realizarse bajo petición o de forma planificada. Las categorías de informes son: i) Crisis de alto nivel (34 informes individuales). ii) Correo por emisor (18 informes individuales). iii) Correo por receptor (18 informes individuales). iv) Spam por emisor (42 informes individuales). v) Spam por receptor (18 informes individuales). vi) Virus por emisor (42

informes individuales). vii) Virus por receptor (18 informes individuales). viii) Estadísticas (tres informes individuales). Así mismo soporta la capacidad de enviar correos de alertas en base a ocho diferentes categorías: incidentes de virus, eventos críticos, disco remoto lleno, fallos en el archivo de correos, eventos de HA, diccionario corrompido, cuota de cuarentena del sistema completa y número de correos postpuestos sobre un período de tiempo

CONSIDERACIONES FINALES

Se ha sometido la presente herramienta durante veinte días a un continuado y exhaustivo conjunto de baterías de ataques, test de seguridad, pruebas de rendimiento, condiciones de fiabilidad y de usabilidad. Los resultados globales han sido del 94,7%.

Se ha podido constatar una capacidad de rendimiento punta de exploración de unos 6,9 millones de correos electrónicos por día. Respecto a sus funcionalidades RAID, se han valorado satisfactoriamente, con posibilidad de soporte de 2,4 Tbytes; también se ha observado una operativa satisfactoria con un número de dominios de correo electrónico de hasta unos tres mil.

En cuanto a las políticas basadas en el receptor (por dominio), se ha constatado la posibilidad de definir hasta 100 políticas para el correo entrante y unas 1.500 para el correo saliente. El número máximo de buzones o cuentas de correo en modo servidor ha sido de 3.000 con cuotas de disco normalizadas. Los números de

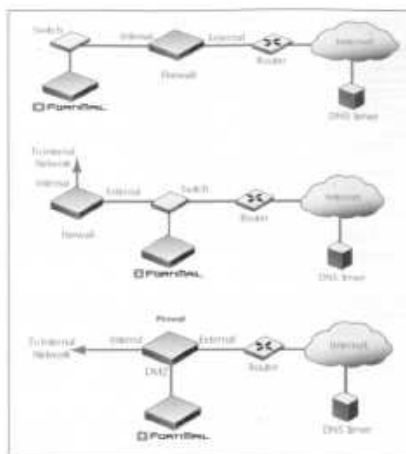


Fig. 10.- Despliegues en modo servidor de la unidad hardware FortiMail-2000A: detrás/delante del cortafuegos y en la DMZ.

perfiles de antispam, de perfiles anti-virus, de perfiles de autenticación, de perfiles de contenido fue de hasta 550. Se ha constatado un soporte de hasta unos 256 alias de correo. El número de dominios de administración añadidos sin inestabilidad fue de cincuenta.

En cuanto al rendimiento medido utilizando RAID 10 ha sido para el encaminamiento de correo de 331.200 mensajes por hora. También se pudieron alcanzar colectivos de hasta unas 512 conexiones SMTP, determinándose una potencia de inspección completa (AV/AS, etc.) entrada/salida del orden de 280.800 correos electrónicos por hora.

Se han utilizado diversas baterías de pruebas de ataques al hardware, al software con resultados globales muy satisfactorios, del orden de un 94,5%. Igualmente, la herramienta de Fortinet se sometió a situaciones de ráfagas y mantenimiento de gran tráfico y estrés con colectivos de

usuarios conectados al servicio de correo de entre cinco y 4.000.000 con funcionamiento estable. La valoración del mecanismo de tolerancia a fallos y alta disponibilidad fue del 89,7%.

Por último, los resultados obtenidos tras las pruebas de ataques *side channels* efectuadas fueron satisfactorios; así, para análisis de *timing*, se logró un 90,1%; para análisis de potencia y DPA (*Differential Power Analysis*), un 91,7%; para análisis de fallos, un 92,7% y para los basados en radiación EM, del 90,2%. Finalmente, la valoración de los mecanismos de gestión de *logs* y de generación de informes fueron del 91,8%, del funcionamiento de las interfaces, del 89,7%, y referente a la fiabilidad de la detección y protección, del 94,7%. ■

CONCLUSIONES

- **OBJETIVO:** herramienta de seguridad de red de naturaleza hardware-software para redes TCP/IP con interfaz LAN Ethernet 10/100/1000 Mbps del tipo sistema especializado de protección multifuncional y multinivel para el servicio de correo electrónico entrante y saliente. Permite hacer frente a todo tipo de ataques y amenazas como *spam*, *phishing*, *virus*, *spyware*, *gusanos*, *bots*, *zombis*, *malware*, *adware*, *DoS/DDoS*, tanto en el cuerpo como en ficheros adjuntos, etc. Incorpora una gestión centralizada rica en funcionalidades. Soporta una gestión de *logs* y una generación de informes muy cuidada. Posibilita una gran flexibilidad en cuanto a modos de despliegue: transparente-puente, pasarela-relay y servidor. Permite almacenar correo y opera con mecanismo de cuarentena.
- **PUNTAJIZACIONES / LIMITACIONES:** los administradores no pueden asociarse con dominios en modo servidor. Permite copiar la configuración de un perfil a un nuevo perfil para crear de forma sencilla gran número de nuevos perfiles. Múltiples perfiles pueden crearse de forma independiente. La opción de cuarentena de correo *spam* no está disponible en el perfil antispam saliente. Los perfiles de autenticación no se aplican a políticas de correo salientes. Soporta autenticación de usuario LDAP en modo servidor. Incluye una utilidad para comprobar un perfil de autenticación basado en LDAP antes de utilizarlo. Soporta autenticación de servidor SMTP. Incluye una libreta de direcciones del sistema en modo servidor. Utiliza *proxies* sofisticados para tráfico SMTP en modo transparente y actúa como un puente desde el punto de vista de la red, pero desde la perspectiva de la aplicación aparece como un cliente o un servidor. Los *proxies* se pueden configurar para tráfico entrante, saliente y local y para cada puerto del hardware FortiMail-2000A. Soporta SMTPS (puerto 465). Los grupos de usuarios se pueden crear por dominio. Si FortiMail no puede enviar correo al servidor SMTP de dominio primario utilizará el computador *MX fallback*. Soporta alias por dominio, así como re-escritura de direcciones de correo. Mete en caché los resultados de todas las búsquedas DNS para mejorar el rendimiento. Los usuarios pueden *resetear/backup/recuperar* sus bases de datos Bayesianas utilizando el GUI Webmail. Soporta SNMP con *traps* como uso CPU/memoria/disco de log/disco de buzones/virus detectados y *spam* detectado. Soporta syslog para descargar datos de log an un servidor remoto. Soporta servidor externo NAS para almacenar la base de datos de correos.
- **IMPACTO DE SU UTILIZACION:** instalación rápida, configuración guiada. Utilización cómoda con niveles de complejidad de básica a alta. Incluye mecanismos de tolerancia a fallos, alta disponibilidad, redundancia e integridad. El rendimiento es muy satisfactorio y la flexibilidad, excelente. Es independiente del número de usuarios y buzones necesarios; da servicio a organizaciones medianas e incluso grandes.
- **PRESTACIONES / VENTAJAS ESPECIALES:** permite configurar el instante y frecuencia de los informes de *spam* en cuarentena. Los procesos de actualización son rápidos y sencillos. Administración directa. Incorpora funcionalidades útiles de registro y diferentes tipos de generación de informes. Soporta la generación, descarga e instalación de certificados SSL para sustituir el certificado SSL por defecto. Integra un exhaustivo conjunto de tecnologías de detección-filtrado: antivirus, antispam, así como un mecanismo de actualización automática, permite una exploración de correos en cabecera, cuerpo, cuerpo en bruto, URI y meta-información. En los modos transparente y pasarela: i) Proporciona navegación basada en acceso a usuarios para procesar correo en cuarentena como *spam*. ii) Proporciona acceso a las preferencias del usuario. iii) Autentica a los usuarios frente a un servidor externo como Radius, LDAP, POP3, IMAP, SMTP. En el modo servidor: a) Proporciona un completo acceso basado en navegador a la cuenta de correo del usuario. b) Proporciona acceso a las preferencias del usuario. c) Autentica a los usuarios sobre una base de datos interna. d) Soporta notificaciones para situaciones de vacaciones y de fuera de la oficina. Proporciona acceso a las libretas de direcciones del sistema y personal. e) Soporta auto-reenvío de nuevos mensajes de correo. f) Permite al usuario importar/exportar su libreta de direcciones personal (en formato CSV). g) Permite al usuario importar/exportar sus listas blanca/ negra personal.
- **DOCUMENTACION:** satisfactoria. Incluye navegador para documentación. Utiliza ficheros .pdf.
- **MODALIDADES DE DESPLIEGUE:** 1) Modo transparente o puente. 2) Modo pasarela o relay. 3) Modo servidor con diferentes ubicaciones: antes/después del cortafuegos y en la zona desmilitarizada o DMZ.
- **CALIFICACION FINAL:** herramienta de seguridad de red flexible, de elevado rendimiento y características de tolerancia a fallos y alta disponibilidad, catalogada como sistema especializado multinivel-multifuncional de protección para el servicio de correo electrónico entrante y saliente. Soporta tres modos de despliegue: transparente, servidor y pasarela. De los tres modos, el modo servidor funciona muy diferente de los modos pasarela y transparente. Con el modo servidor, el *appliance* es el servidor de correo donde se ofrecen los medios para explorar el tráfico de correo. Con los modos pasarela y transparente, el *appliance* se sitúa entre el *firewall* y el servidor de correo y actúa como un filtro para el correo que pasa a través de él. Dependiendo de cómo se ejija el despliegue del *appliance* se determina cual de los modos es más adecuado para su entorno. En todos los modos el *appliance* explora el tráfico de correo en busca de virus, *spam*, *phishing*, etc. y puede poner en cuarentena correo y adjuntos sospechosos. Integra un rico conjunto de funcionalidades de detección y actuación contra *spam*, *malware*, *phishing*, *gusanos*, *spyware*, ataques *DoS/DDoS*, etc. Se gestiona de forma centralizada desde GUI y/o CLI, destacando los mecanismos de políticas, la gestión de *logs* y la cuidada generación de informes.

EQUIPO DE EVALUACIÓN

DIRECTOR:
 Prof. Dr. Javier Areitio Bertoín
 Catedrático de la Facultad de Ingeniería. ESIDE.
 Director del Grupo de Investigación Redes y Sistemas.
 UNIVERSIDAD DE DEUSTO

