



Fortinet FortiOS 4.0

Control, optimización e inspección de redes

En colaboración con **TCN**

El sistema operativo FortiOS para dispositivos de seguridad multi-amenaza FortiGate de la compañía Fortinet se ha actualizado, con la incorporación de la versión 4.0, que integra cientos de nuevas características, ofreciendo una combinación amplia y potente de seguridad y servicios de red en una plataforma única e integral.

El proveedor de seguridad de redes y líder mundial de soluciones de gestión unificada de amenazas –UTM– Fortinet, ha dado a conocer el nuevo sistema operativo FortiOS en su versión 4.0. Esta importante actualización del firmware integra cientos de nuevas características para mejorar significativamente el valor y funcionalidades de sus dispositivos de seguridad multi-amenaza FortiGate. Además, con FortiOS 4.0 la firma ofrece a sus clientes una combinación ampliada y potente de los servicios de seguridad y de red, todo ello en una plataforma única e integral, que ayuda a las empresas a proteger toda su infraestructura corporativa.

CARACTERÍSTICAS

Entre las principales características de esta nueva revisión del sistema operativo FortiOS 4.0 se encuentran el control de aplicaciones, la protección de fuga de datos o DLP, la optimización de las redes WAN, y la inspección de tráfico SSL. Este conjunto de funcionalidades aporta a los appliances FortiGate mayor seguridad y mejor rendimiento de la red corporativa.

El control de aplicaciones se encarga de reconocer el tráfico de la aplicación que

lo está generando, en vez del puerto o protocolo observado, con lo que se consigue reforzar las políticas de seguridad para más de mil aplicaciones existentes en el mercado, facilitando el control sobre las mismas. Por otro lado, el sistema de prevención de fuga de datos ayuda a las empresas a identificar y prevenir la comunicación de información sensible fuera de los límites de la red, con lo que se mejora sustancialmente la seguridad. Esta herramienta trabaja a través de cualquier aplicación, incluso cuando el tráfico está encriptado en SSL, proporcionando adicionalmente auditoría para datos y archivos, a la vez que ayuda a cumplir con las normativas vigentes en la protección de datos.

Otra de las principales características de FortiOS 4.0 es la optimización WAN, que acelera las aplicaciones sobre las conexiones WAN, con lo que se consigue incrementar el rendimiento de la red, disminuyendo los requisitos de ancho de banda y de recursos del servidor. Todo esto se traduce en una mejora de la productividad de los usuarios, a la vez que se produce un ahorro de los costes de las redes. Simultáneamente, la inspección SSL

aumenta la seguridad y políticas de control entre los flujos de tráfico encriptados, con lo que se consigue mejorar la protección cuando se navega por Internet, así como de los servidores de aplicaciones.

MEJORES DEFENSAS

En su conjunto, estas cuatro principales características de FortiOS 4.0 ayudan a las empresas a mejorar sus defensas, obteniendo más valor por su inversión, y mejoras en la eficacia de la gestión de todos los sistemas. Entre los principales beneficios para los clientes que implementen esta solución, se encuentran: acceso a nuevas e innovadoras tecnologías de seguridad, mejor integración con todas las tecnologías existentes, control sobre los usuarios locales que se comunican a través de un mayor número de aplicaciones basadas en web, y la reducción del número de dispositivos físicos necesarios para implementar la seguridad y los servicios de red deseados.



FUNCIONALIDADES

- Mejoras en la seguridad y el rendimiento de la red
- Control de aplicaciones
- Prevención de fuga de datos
- Optimización WAN
- Inspección SSL





Iberia FortiPartner Conference 2009

Con sesiones comerciales y técnicas, el próximo 29 de abril se celebrará Iberia FortiPartner Conference 2009, donde se ofrecerá la oportunidad de compartir los planes para asegurar el éxito de los clientes y partners de Fortinet. Además, se podrá compartir la más actualizada información acerca del mercado de seguridad, así como los últimos productos, soluciones y herramientas para conseguir mejorar las infraestructuras, implementando las soluciones de Fortinet.

Durante todas las sesiones, los principales representantes del equipo directivo de Fortinet Iberia compartirán los planes de futuro, las innovadoras soluciones y el programa de canal que otorga a sus socios muchas ventajas competitivas con respecto a otros fabricantes.

*Madrid 29 abril. Casa de Mónico
(Ctra. de la Coruña km 9,5)*

Para más información: www.fortinet-ipc2009.es

TÉCNICAS EMPLEADAS

Entre las principales técnicas empleadas por esta solución se encuentran: Web Caching –acelera transacciones con aplicaciones web reduciendo la carga de los servidores web y el ancho de banda–; Protocol Optimization –mejora el uso del ancho de banda y la eficiencia de la comunicación–; Byte Caching –fragmenta paquetes de datos en unidades más pequeñas, con lo que se consigue agilizar la transferencia de ficheros–; aceleración SSL –con los circuitos ASIC CP6 de última generación se acelera el cifrado/descifrado de tráfico SSL–; Secure Tunneling entre WAN Peers –empleando túneles SSL se garantiza la privacidad de las comunicaciones dentro del túnel WAN–; Data Leak Protection –protege de fuga de datos los diferentes proto-

colos de transferencia–; detección de intrusos –protección más robusta contra ataques DoS, filtrado de tráfico, opciones de cuarentena, etc.–; End Point Compliance –integración de la capa firewall perimetral con el puesto de trabajo–; y balanceo de servidores –permite realizar balanceos de una VirtualIP publicada en servidores internos mediante diferentes criterios–.

Además, también incluye soporte SNMPv3, posibilidad de crear reglas any to any, mejoras en traffic shaping, recursos configurables por vdom, utilización de puertos no estándar para la autenticación, comunicación soportada con servidores OSCP y SCEP, filtrado de actividades HTTP POST, y asignación de IP a clientes VPN mediante Radius.

La estabilidad financiera de Fortinet, ajena a la crisis económica

Fortinet ha anunciado sus resultados financieros y corporativos del cuarto trimestre de 2008, así como del año fiscal finalizado el 28 de diciembre de 2008. Según responsables de la compañía, la fuerte demanda de dispositivos de seguridad ha consolidado su evolución, y muestra de ello

es el aumento de sus ingresos durante el cuatro trimestre de 2008, con respecto al mismo periodo del año anterior: un 35%, hasta alcanzar los 59 millones de dólares. Por otro lado, la facturación también ha crecido en un 31%, llegando a los 73 millones de dólares. En cuanto los datos correspon-

dientes a Iberia en el último trimestre de 2008, la filial ha obtenido un incremento global del 52%, en comparación al mismo periodo del año anterior.

Siguiendo con los resultados financieros correspondientes al año fiscal 2008, Fortinet creció un 36% en ingresos –212

millones de dólares–, y un 30% en facturación –252 millones de dólares–. Unas cifras que también se reflejan en el último informe IDC Worldwide Quarterly Security Appliance Tracker, que confirma a Fortinet como líder en ingresos de UTM durante el tercer trimestre de 2008.

Técnicas Reunidas selecciona a Fortinet para dotar de seguridad a sus redes



TECNICAS REUNIDAS

Técnicas Reunidas, contratista general internacional que se dedica a la ingeniería y construcción de instalaciones industriales para petróleo y gas, refino y petroquímica, energía, infraestructuras e industria, ha desplegado un completo y flexible servicio de protección con dispositivos de Fortinet para garantizar la seguridad de los más de 4.000 usuarios de sus distintas redes internas.

La protección de su perímetro era uno de los mayores retos a los que se enfrentaba la organización. Técnicas Reunidas contaba con dos barreras firewall, sin embargo la barrera externa presentaba distintos problemas, principalmente de estabilidad y gestión. Éste fue el punto a partir del cual decidieron emprender un proyecto para el reemplazo de dicha barrera de seguridad perimetral. La compañía necesitaba una solución con una gestión sencilla de las políticas de seguridad, que soportase NAT y ofreciese la posibilidad de filtrar e inspeccionar su tráfico de navegación (navegación limpia).

El objetivo del proyecto era encontrar una solución como primera barrera de seguridad perime-



tral robusta con una gestión sencilla de políticas de seguridad y NAT. Tras testar en producción varias soluciones de la industria, Técnicas Reunidas finalmente eligió dos clusters FortiGate 3016B en Bundle (incluyendo todos los servicios de seguridad FortiGuard) para su sede principal y de transmisión de datos a nivel mundial. Las razones princi-

pales de dicha decisión fueron su facilidad de gestión, los altos niveles de efectividad y el alto rendimiento proporcionado.

Por otra parte, otro de los apartados abarcados por el proyecto ha sido el relativo al filtrado de la navegación por Internet, ya que la organización carecía de una solución que protegiese la navegación de los más

de 4.000 puestos de trabajo de sus distintas redes internas, que generan un muy elevado tráfico HTTP, de forma sencilla e integrada.

EVALUACIÓN

Frente a este marco, y ante la necesidad de garantizar la seguridad en la navegación, y delimitar el acceso a determinadas páginas potencialmente peligrosas o improproductivas, se abrió un proceso de evaluación de distintas herramientas del mercado capaces de proporcionar los altos niveles de seguridad y rendimiento requeridos para proteger el tráfico, siendo uno de los principales requisitos de Técnicas Reunidas que la solución finalmente elegida no introdujese retardos apreciables en la navegación. Después de las pruebas en producción con numerosos fabricantes, Fortinet fue nuevamente elegido por su gran nivel de eficacia de detección de virus y malware en el tráfico de navegación, por su elevado nivel de eficiencia de categorización de los sites de Internet y por el alto rendimiento demostrado durante las pruebas en comparación con el resto de fabricantes. Con la implementación de VDO-Ms (virtualización de equipos) se alcanzó la reducción de costes y se cubrieron con una única plataforma todos sus requerimientos de seguridad, para todos los usuarios de la organización.