

# Soluciones de Seguridad

## FortiGate



## ÍNDICE

<a href="#">1. Introducción .....</a>	<a href="#">3</a>
<a href="#">2. ¿Por qué Fortinet? .....</a>	<a href="#">4</a>
<a href="#">2.1 Equipamiento de alto rendimiento .....</a>	<a href="#">4</a>
<a href="#">2.2 Servicios Fortinet .....</a>	<a href="#">4</a>
<a href="#">3 Características técnicas de los equipos .....</a>	<a href="#">4</a>
<a href="#">3.1 La arquitectura Fortigate .....</a>	<a href="#">4</a>
<a href="#">3.2 Alta disponibilidad .....</a>	<a href="#">5</a>
<a href="#">3.3 Virtualización .....</a>	<a href="#">5</a>
<a href="#">3.4 Networking .....</a>	<a href="#">5</a>
<a href="#">3.5 Balanceo .....</a>	<a href="#">6</a>
<a href="#">3.5.1 Balanceo de carga.....</a>	<a href="#">6</a>
<a href="#">3.6 Calidad de servicio .....</a>	<a href="#">6</a>
<a href="#">3.7 VPN .....</a>	<a href="#">6</a>
<a href="#">3.8 Antivirus .....</a>	<a href="#">7</a>
<a href="#">3.9 IDS / IPS .....</a>	<a href="#">7</a>
<a href="#">3.10 AntiSpam.....</a>	<a href="#">8</a>
<a href="#">3.11 URL Filtering.....</a>	<a href="#">9</a>
<a href="#">4. Sistema de gestión.....</a>	<a href="#">9</a>
<a href="#">5. Sistema de logging y reporting .....</a>	<a href="#">10</a>
<a href="#">6. Nuevas funciones FortiOS 4.0 .....</a>	<a href="#">10</a>

## 1. INTRODUCCIÓN

Fortinet fue fundada en el año 2000 por Ken Xie, visionario y previo fundador y CEO de NetScreen. En su etapa en NetScreen, Ken Xie fue pionero en la utilización de un Circuito Integrado de Aplicación Específica (ASIC) para acelerar el proceso Firewall. De este modo lanzó al mercado un lineal de equipos de alto rendimiento que mediante aceleración hardware permitía realizar un control sobre el tráfico de las redes en tiempo real, que tuvo inmediatamente una gran acogida en el mercado.

Ken Xie, con objeto de seguir avanzando en su visión propia de la seguridad en las comunicaciones, abandonó NetScreen y fundó Fortinet. Su proyecto consistía en dar un enorme paso más en la seguridad en tiempo real, integrando antivirus, filtrado de contenido, tecnología IDP (Intrusion Detection and Prevention) y Antispam en un solo dispositivo, junto con el firewall y servidor VPN, y acelerando esta Protección Completa de Contenidos mediante un nuevo ASIC, FortiASIC, que permite romper la barrera del procesado de contenidos en tiempo real.

Algunas de las características más destacables de Fortinet son las siguientes:

- Presencia mundial de sus centros de operación, ventas y soporte
- Sede central en Sunnyvale, California
- Más de 75.000 clientes en todo el mundo con más de 450.000 equipos instalados
- Más de 40 oficinas en América, Asia y EMEA, con sede central europea en Sophia-Antipolis (Francia)
- Pioneros en la utilización de Circuitos Integrados de Aplicación Específica para acelerar los procesos de seguridad hasta el nivel de aplicación
- Único modo de ofrecer Protección Completa en Tiempo Real
- Líderes en el mercado UTM (Unified Threat Management) según IDC desde el 2003 hasta el 2009
- Tecnologías certificadas ICSA (6 certificaciones), NSS (UTM), ISO 9001:2000, Common Criteria EAL4+ y FIPS-2.
- Robusto apoyo financiero

Fortinet es la compañía de seguridad de más rápido crecimiento en la historia. Desde su entrada en el mercado, anualmente ha duplicado su penetración en el mismo así como sus beneficios, con una inversión en I+D+I constante.

## **2. ¿Por qué Fortinet?**

### **2.1 Equipamiento de alto rendimiento**

Los equipos de seguridad Fortinet constituyen una nueva generación de equipos de seguridad de muy alto rendimiento que garantizan la protección completa de nuestros sistemas en tiempo real.

La serie FortiGate, que ofrece altísimos niveles de escalabilidad, rendimiento, seguridad y flexibilidad de despliegue, es la única plataforma de Gestión Unificada de Amenazas (UTM- Unified Threat Management) que cuenta con seis certificaciones ICASA y que además cumple el estándar ATCA –Advanced Telecom Computing Architecture–, integrando una completa gama de funciones y servicios de seguridad para proteger las redes de las sofisticadas amenazas combinadas. Entre las funcionalidades integradas de estas plataformas de Gestión Unificada de Amenazas –UTM– se incluyen cortafuegos de inspección de estado, VPN IPSec y SSL, detección y prevención de intrusiones, filtrado de contenido web, antispam, antivirus, controles de mensajería instantánea y controles P2P (peer-to-peer). Estos servicios de seguridad funcionan conjuntamente para prevenir que los ataques mixtos afecten a la red.

### **2.2 Servicios Fortinet**

Fortinet ofrece de forma conjunta con su equipamiento servicios profesionales que garantizan el soporte, la actualización y el correcto mantenimiento de los niveles de servicio demandados. Gracias a los equipos técnicos distribuidos a lo largo de todo el mundo, Fortinet es capaz de ofrecer soporte internacional con cobertura 24x7x365, actualizando en tiempo real las bases de datos de firmas de antivirus e IDS/IPS y los motores de estas aplicaciones, así como actualizando de forma continuada las bases de datos en las que se apoyan los servicios Fortiguard Web Filtering y Fortiguard AntiSpam.

El Servicio FortiProtect Distribution Network (FDN) se encarga de la distribución de estas actualizaciones a lo largo de todo el mundo, existiendo el compromiso con aquellos clientes que contratan el servicio FortiProtect Premier Services de disponer de la firma correspondiente a cualquier nuevo ataque en menos de 3 horas.

## **3 Características técnicas de los equipos**

### **3.1 La Arquitectura FortiGate**

La tecnología Fortinet es una poderosa combinación de software y hardware basada en el uso de "Circuitos Integrados de Aplicación Específica", conocidos por sus siglas en inglés como ASIC, a través de la cual es capaz de ofrecer el procesamiento y análisis del contenido del tráfico de la red sin que ello suponga ningún impacto en el rendimiento de las comunicaciones.

La tecnología incluye el Procesador FortiASICTM y el Sistema Operativo FortiOSTM los cuales forman el núcleo de los equipos FortiGate y son la base del alto rendimiento ofrecido por los equipos.

### 3.2 Alta disponibilidad

Conjunto de dos o más máquinas que se caracterizan por mantener una serie de servicios compartidos y por estar constantemente monitorizándose entre sí.

*Activo-Activo (en modo router y transparente):* La configuración de "alta disponibilidad" en activo-activo es muy similar a la de activo-pasivo, aunque en este caso los dos nodos comparten los servicios de una manera activa, normalmente balanceados, consiguiendo una disponibilidad mayor ya que los servicios se entregan antes.

*Pasivo-Activo:* Se trata de disponer de un nodo funcionando, contando con todos los servicios que componen el sistema de información al que denominaremos Activo, y el otro nodo que se denominará Pasivo en el que se encuentran duplicados todos estos servicios, pero detenidos a espera de que se produzca un fallo.

### 3.3 Virtualización - VDOMs

Los equipos FortiGate permiten la utilización de Dominios Virtuales, de modo que sobre una única plataforma física podemos configurar hasta 500 Equipos virtuales, completamente independientes entre sí y con todas las funcionalidades que posee cada plataforma física. Todos los equipos FortiGate disponen en su configuración básica de la capacidad de definición de hasta 10 dominios virtuales, siendo posible ampliar el número de éstos en los equipos de gama alta (a partir de la gama FG3000), llegando hasta 500 Dominios Virtuales.

Cada uno de estos dominios virtuales representan de forma lógica una máquina independiente del resto, asignándoles interfaces lógicas (VLAN's) o físicos con la posibilidad de trabajar en modo router o transparente, aplicar diferentes perfiles y políticas sobre cada máquina, etc.

### 3.4 Networking

La línea de soluciones de seguridad multiamenaza FortiGate Series ofrece a las empresas un sencillo despliegue, al permitir su instalación sin problemas en redes de última generación.

- *Modos de Operación:*
  - Modo NAT
  - Modo transparente: Se coloca delante del servidor 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 puente.
- *Soporte PPPoE (Protocolo Punto a Punto sobre Ethernet)*
- *Soporte DDNS support*
- *DHCP for Branch Office*
- *Proxy DNS*
- *Protocolos de Routing: Static, RIP v1 and v2, OSPF*
- *SNMP Support*
- *Posibilidad de personalización de los mensajes mostrados a los usuarios relativos a cada una de las funcionalidades*
- *ICSA Certification*
- *Stateful Inspection (Inspección profunda de paquetes)*

- *Virtual IP*
- *802.1q VLAN support*
- *Políticas de autenticación basadas en grupos de usuarios*
- *Autenticación externa: RADIUS, LDAP*
- *Proceso acelerado por ASIC*

### **3.5 Balanceo**

Suministra una completa solución de acceso remoto que consolida la aceleración WAN, VPN y multi-homing para garantizar una conectividad rápida y fiable de las operaciones remotas y acceso global seguro a las aplicaciones distribuidas que se encuentran en el centro de datos. Soporta balanceo estático de ISPs y políticas basadas en rutas (policy routing) con la posibilidad de enrutar los paquetes por cualquier otro dato que no sea la dirección destino del paquete.

#### **3.5.1 Balanceo de carga**

Los dispositivos FortiGate permiten la configuración de IP's virtuales (VIP's) de manera que estas ofrecen balanceo de carga de servidores, teniendo la capacidad de que las peticiones realizadas a la IP virtual puedan ser atendidas por un grupo de servidores habilitados para ese efecto. La distribución del balanceo de carga puede ser configurado a nivel de puertos TCP o UDP, con la posibilidad de tener varios servicios desplegados en la misma IP y atendidos por grupos de servidores distintos. Cada uno de los servidores que componen grupo de balanceo, puede ser monitorizado a nivel ICMP, TCP o http de manera que ante el fallo de un servidor, el servicio continúa activo en el resto de equipos, dotando a la plataforma de alta disponibilidad.

### **3.6 Calidad de servicio**

#### *Traffic shaping*

El **Traffic shaping** o catalogación de tráfico controla el tráfico en redes de ordenadores para así lograr optimizar o garantizar el rendimiento, baja latencia, y/o un ancho de banda determinado, pudiendo priorizar políticas de firewall por:

- Ancho de banda garantizado
- Ancho de banda máximo
- Priorización dinámica entre políticas

### **3.7 VPN**

Los equipos FortiGate soportan el establecimiento de Redes Privadas Virtuales basadas en protocolos IPSec y SSL, además de PPTP. De esta forma, oficinas pequeñas, medias, corporaciones e ISPs pueden establecer comunicaciones privadas sobre redes públicas garantizando la confidencialidad e integridad de los datos transmitidos por Internet. Al estar integrada la funcionalidad VPN en la propia plataforma FortiGate, el tráfico VPN puede ser analizado por el módulo de Firewall así como por las funcionalidades adicionales antivirus, IPS, web filtering, antispam, etc.

Algunas características son:

- Soporte para VPN Site-to-Site, en modo router y transparente.
- Soporte para VPN cliente en modo router y transparente

- Soporte DDNS.
- Soporte DES, 3DES, AES256, L2TP, PPTP
- Load Sharing e clustering
- Gestión de Certificados Digitales
- Autenticación externa (Radius, LDAP)
- Nat /Pat
- Xauth sobre Radius
- Internet Key Exchange (IKE)
  - Diffie-Hellman (DH) Groups 1, 2, 5
  - RSA Certificates
- Protocolos de routing RIP, RIP2, OSPF
- IPSEC Nat transversal
- Dead peer detection
- DHCP sobre IPSEC
- Soporte para VPN Hub and Spoke
- Proceso acelerado por ASIC

### 3.8 Antivirus

La protección Antivirus se encarga de detectar, desinfectar y/o eliminar de códigos maliciosos a la empresa, con actualizaciones en tiempo real para proteger contra nuevos ataques. Certificado por ICSA Network Antivirus es capaz de analizar los siguientes protocolos: HTTP, FTP, SMTP, POP3, IMAP y posibilidad de buscar virus en cualquier otro puerto distinto al de por defecto para estos protocolos y basada en firmas.

Características:

- Soporte de escaneo del tráfico de los túneles IPSEC terminados en el dispositivo.
- Posibilidad de update de firmas en modo Push y Pull
- Heuristic detection
- Grayware detection
- Spyware detection
- Block by file size and Type
- Posibilidad de cuarentena automática
- Posibilidad de redirección de los ficheros infectados para análisis
- Soporte de ficheros comprimidos ZIP, LHA, LZH , ARJ, CAB, TAR, GZ, RAR, incluso anidados
- Proceso acelerado por ASIC
- Funcionalidad proporcionada por el mismo fabricante del equipo CPE

### 3.9 IDS/IPS

Detección y Prevención de Intrusión es un sistema que se encarga de la detección y prevención automática, y en tiempo real, de más de 4.000 tipos de ataques. Esto permite a la Seguridad FortiGate parar los ataques que evaden los sistemas de antivirus convencionales a base de anfitrión, y proporciona la respuesta inmediata a amenazas de extensión rápidas. Usando la Red de Distribución global FortiGuard, FortiGate para los ataques más perjudiciales en el perímetro de red independientemente de si la red es cableada, inalámbrica, etc. Además la tecnología única de Fortinet también apoya la heurística a base de comportamiento que añade capacidades de reconocimiento valuosas más allá simplemente de la correspondencia del contenido contra firmas conocidas

Proceso acelerado por ASIC y certificado por ICSA cumple las siguientes características:

- Soporte de escaneo del tráfico de los túneles IPSec terminados en el dispositivo.
- Posibilidad de update de firmas en modo Push y Pull
- Posibilidad de creación de firmas
- Detección de anomalías de protocolo
- Basado en estadísticas
  - Flooding - If the number of sessions targeting single destination in one second is over a threshold, the destination is experiencing flooding.
  - Scan - If the number of sessions from a single source in one second is over a threshold, the source is scanning.
  - Source - If the number of concurrent sessions from a single source is over a threshold, the source session limit is reached.
  - Destination session limit - If the number of concurrent sessions to a single destination is over a threshold, the destination session limit is reached.
- Anomalías de protocolos: Check packets and sessions for conformance to Internet standards

### 3.10 AntiSpam

La funcionalidad AntiSpam ofrecida por los equipos FortiGate consiste en la aplicación de diferentes filtros sobre el tráfico de intercambio de correo electrónico (protocolos SMTP, POP3 e IMAP). Aquellos filtros que requieren la conexión con servidores externos (FortiGuard Antispam o los servicios de Listas Negras en tiempo real) se ejecutan de forma simultánea con los otros filtros, optimizando el tiempo de respuesta del análisis de los mensajes. Tan pronto como alguno de los filtros aplicados identifica el mensaje como spam se procede a realizar la acción definida para cada filtro que podrá ser:

- Marcar el mensaje como Spam (Tagged): El mensaje quedará identificado como Spam, y en el perfil de protección podremos decidir si se deja pasar, identificándolo como Spam y pudiendo incluir en la cabecera del mismo o en el encabezamiento MIME un mensaje identificativo, o bien si preferimos descartar el mensaje (solo sobre SMTP).
- Descartar (Discard): En este caso el mensaje es desechado, en el caso de SMTP es posible sustituirlo con un mensaje predefinido que advierta al usuario del envío de Spam.

Los filtros antispam aplicados por la plataforma FortiGate a los mensajes de correo se basan en el control por origen del mensaje y el control por el contenido del mismo.

- Source control
  - By email addresses
  - By Mail server IP address
- Static lists (locally maintained on the FortiGate)
- Dynamic lists (real-time DNS blacklists available on the Internet)
- HELO DNS lookup (SMTP)
- Content Control
  - MIME Headers
  - Banned words lists
- AntiSpam managed Service (FortiGuard AntiSpam)
  - Open Relay Data base
  - URI Database

### 3.11 URL Filtering

El Servicio de Filtrado Web de Fortinet entrega actualizaciones para regular actividades web. Con 75 categorías de contenidos web, más de 30 millones de sitios web nominales y más de dos mil millones de páginas web, el Servicio de Filtración de FortiGuard es uno de los servicios integrados más exacto de la industria.

La solución Fortiguard Web Filter consiste en dos partes, los Servidores Fortiguard y el sistema de seguridad multiamenaza FortiGate. Los servidores FortiGuard contienen una base de datos de posiciones que consiste en unos mil millones de direcciones de páginas web. El servicio de Filtración FortiGuard puede ser activado sobre todos los sistemas de seguridad FortiGate para regular y bloquear el acceso a los sitios web dañinos, inadecuados y peligrosos que pueden contener ataques de Phishing y/o malware como spyware. Las posibilidades de filtrado son múltiples:

- Filtrado de URL
  - Por direcciones IP
  - URLs completas
  - URLs definidas usando wildcards o regular expressions.
  - Posibilidad de importar listas de terceros
- URL Exempt list
- Filtrado de contenido - Listas negras/blancas locales
- Filtrado de Scripts - Java applets, cookies, y activeX
- URL Filtering managed Service (FortiGuard)
  - More that 25 Million Domains categorized
  - 56 categories

## 4. Sistema de Gestión

Una vez instalada la unidad hardware se puede configurar y gestionar. Además se posibilita la administración basada en roles para multiples administradores con funciones dedicadas.

Las formas de gestión son:

*Gestor basado en Web:*

Es posible configurar, gestionar y monitorizar el estado de la unidad hardware utilizando http, https (mejor opción) a través de un computador que opere en red. Los cambios de configuración son efectivos de forma inmediata.

*Interfaz de linea de comandos ó CLI:*

Se puede conectar al puerto serie de un pc de gestión al conector DB9 de consola serie. 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.

*Actualizaciones automáticas:*

Servicios de Suscripción de Seguridad FortiGuard, permite la protección de red

actualizada 24x7 frente a todo tipo de amenaza.

Actualmente, más de 135.000 sistemas UTM FortiGate cubren en tiempo real en todo el mundo las amenazas de seguridad basadas en contenido de las actuales redes corporativas que han rebasado las capacidades de las tradicionales defensas basadas en cortafuegos.

## **5. Sistema de logging y reporting**

- 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.
- Centralización de logs:  
Posibilidad de almacenar eventos en memoria, discos duros ó envío de información a un sistema de Syslog externo o Fortianalyzer.
- El archivado de contenidos permite guardar información relevante: SMTP, POP3, FTP, HTTP, IM
- Espacio reservado para cuarentena de antivirus.
- Alertas por email para eventos críticos.

## **6. Nuevas funciones FortiOs 4.0**

### **6.1 Fortinet wan acceleration**

La opción de WAN Acceleration está pensada para mejorar e incrementar rendimiento y seguridad en comunicaciones a través de redes de área extensa, como puede ser el caso de Internet o MacroLans.

### **6.2 Web caching**

Básicamente se aceleran transacciones con aplicaciones WEB reduciendo la carga de dichos servidores web y el ancho de banda utilizado, así como la percepción de latencia por el usuario final.

### **6.3 Aceleracion ssl**

Gracias a los circuitos ASIC CP6 de última generación se acelera el cifrado/descifrado de tráfico SSL.

### **6.4 inspeccion de contenido y analisis en comunicaciones ssl**

Básicamente se lleva a cabo una arquitectura del tipo 'man-in-the-middle' y de esta forma se permite inspeccionar contenidos (por ejemplo detectar un virus) en comunicaciones tunelizadas sobre SSL como HTTPS,SMTPS,POP3S o IMAPS.

### **6.7 Data leak protection**

Protección de fuga de datos en diferentes protocolos de transferencia de datos utilizados usualmente (smtp,ftp,http...) con reglas o grupos de reglas predefinidas (por ejemplo una de ellas inspecciona en busca de números de tarjetas de crédito) o totalmente personalizables.

## **6.8 Control de aplicaciones**

Control de tráfico basándose en las aplicaciones que lo generan y con independencia del puerto utilizado. Antes ya se contaba con controles para algunos protocolos (sobre todo P2P e IM) ahora se han incluido controles para mas protocolos/aplicaciones con independencia del puerto por lo que se ha realizado un apartado especial para este control de aplicaciones.

## **6.9 End point compliance**

Integración de la capa firewall perimetral con el puesto de trabajo. Mediante Forticlient es posible securizar los puestos de trabajo (AV,IPS,AP,WF) dentro y fuera del entorno laboral. En el entorno laboral se pueden aplicar las políticas de seguridad de Firewall perimetral basándose en el grado de seguridad que el puesto de trabajo concreto necesita gracias a Forticlient. Se pueden aplicar unas u otras políticas de seguridad y dar al Firewall información del puesto de trabajo tal como Hostname, IP, volumen de tráfico generado en KB, versión del SSOO, Dominio, tipo de CPU, memoria etc...