Ciberseguridad

FIREWALL AVANZADO FORTIGATE

Gigas incorpora en su Cloud DataCenter tecnología Fortinet, fabricante líder en soluciones de seguridad perimetral avanzada con una probada experiencia en la protección de la información, control, inspección y gestión multi capa del tráfico, en estricto cumplimiento con las exigencias de las más grandes corporaciones.

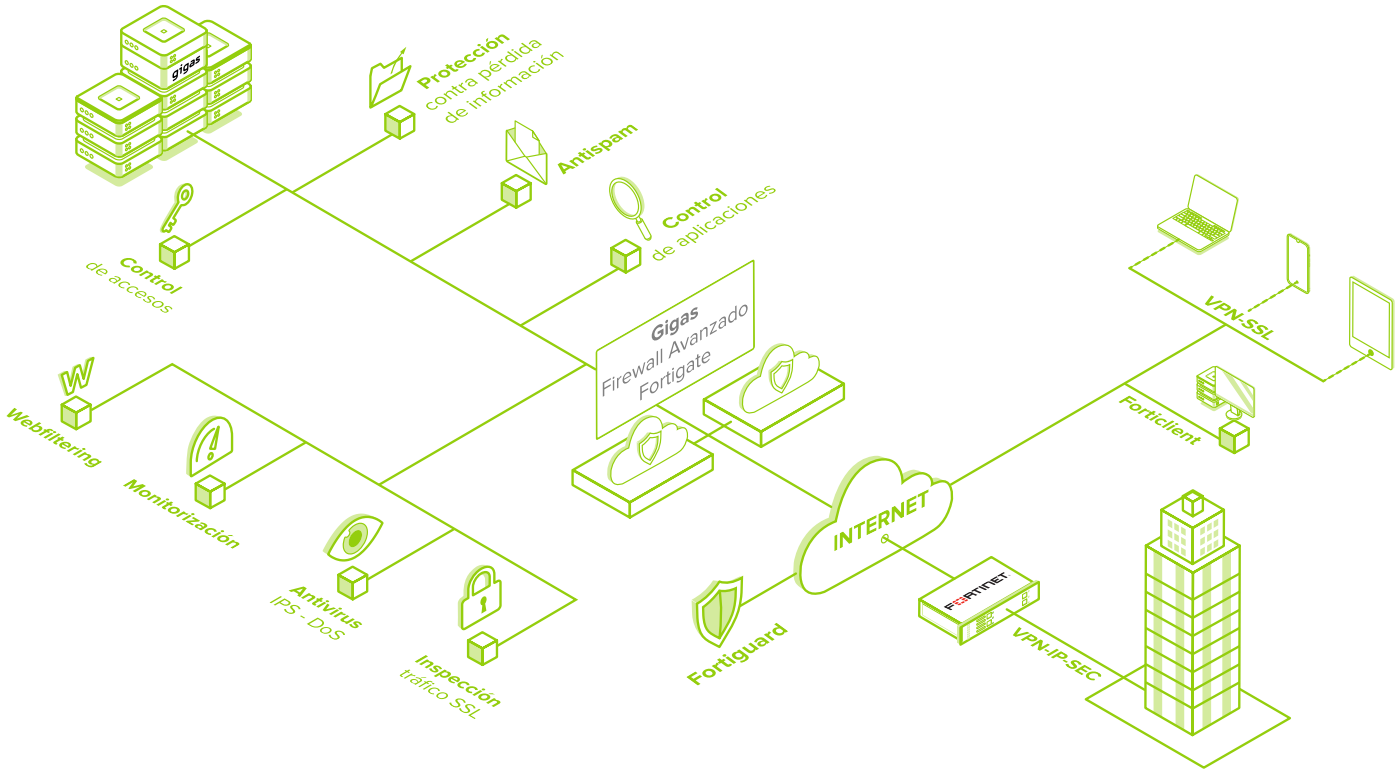
El Firewall Avanzado Fortigate de Gigas ofrece a los usuarios Cloud DataCenter una solución integral de seguridad, sobre Fortigate VM, que resuelve las necesidades fundamentales de protección, control de la información y acceso a los recursos Cloud. Además de garantizar una integración segura del entorno Cloud con las plataformas originales de los usuarios y sus necesidades de movilidad, el Firewall Avanzado Fortigate de Gigas permite simplificar las labores de gestión de sus políticas particulares de seguridad, desde una gestión centralizada e integral multi-plataforma.

Gigas cuenta con equipo propio de Ingeniería, a disposición de nuestros clientes las 24h del día, durante los 365 días del año, que además de velar por el bienestar de la plataforma, libre de amenazas e intrusiones que puedan interferir sobre la calidad de nuestros servicios, pueden asumir la administración delegada del Firewall Avanzado Fortigate que requieran nuestros clientes.

Gigas ofrece trials gratuitos de su Firewall. Si estás interesado escríbenos a info@gigas.com

BENEFICIOS

- **Protección total de la red y la información**
- **Instalación inmediata**
- **Uso eficiente de recursos**
- **Más Inteligencia: “Smart policies”**
- **Tecnología líder**
- **Pruébalo antes de forma gratuita**



MÓDULOS

Módulo Firewall
La tecnología Firewall de Fortinet ofrece inspecciones de tráfico multicapa desde una gestión integral de la solución con altas prestaciones de seguridad. Combina motores para el Control de aplicaciones, antivirus, IPS, filtrado Web, antispam y VPN, junto con avanzadas funcionalidades como una base de datos de amenazas con actualizaciones automatizadas, gestión de vulnerabilidades y una inspección basada en flujos, para identificar y mitigar las últimas y más complejas amenazas.
El sistema operativo FortiOS está creado para la inspección e identificación de malware.

Características:
- NAT, PAT y Transparente (Bridge)
- NAT basado en políticas
- SIP/H.323/SCCP NAT Transversal
- VLAN Tagging (802.1Q)
- Gestión de vulnerabilidades
- Soporta IPv6

Módulo de Control de Accesos Endpoint NAC
Este módulo puede forzar el uso de políticas de seguridad en usuarios conectados a su red corporativa. El módulo verifica la instalación, operaciones de firewall y actualizaciones de firmas del antivirus, antes de permitir el acceso a la red de los nuevos clientes. Permite poner en cuarentena aquellos servidores con aplicaciones que no cumplan con las normas de seguridad.

Características:
- Monitorización y control de servidores operando con FortiClient
- Escaneo de vulnerabilidades de Nodos de Red
- Portal de cuarentena
- Control y detección de aplicaciones
- Base de datos de aplicaciones predefinidas

Módulo Antivirus / Antispyware
La tecnología de inspección de contenido antivirus protege contra virus, spyware, gusanos, y otros tipos de malware que pueden infectar la infraestructura de red y los dispositivos de usuarios. Mediante la intercepción e inspección del tráfico y del contenido en capa 7, la protección del antivirus asegura que las amenazas ocultas maliciosas a nivel de aplicación sean identificadas y eliminadas del flujo de datos, antes de que puedan causar algún daño. El servicio de suscripción FortiGuard asegura que los dispositivos estén actualizados con las últimas firmas malware para altos niveles de detección y atenuación.

Características:
- Actualizaciones automáticas de bases de datos
- Antivirus basado en Proxy
- Antivirus basado en flujos
- Archivo de cuarentena
- Soporta IPv6

Módulo de Prevención de intrusiones IPS
La tecnología IPS protege, contra amenazas actuales y emergentes. Además de detección de amenazas basadas en firmas, IPS realiza detección de anomalías las cuales alertan a los usuarios de cualquier tráfico que coincida con perfiles de comportamiento de ataque. El equipo de búsqueda de amenazas de Fortinet analiza comportamientos sospechosos, identifica y clasifica amenazas emergentes, y genera nuevas firmas para incluir en las actualizaciones FortiGuard.

Características:
- Actualizaciones automáticas de la base de datos
- Soporta anomalías en protocolos
- Sensor de prevención IPS y DoS
- Soporta la personalización de firmas
- Soporta IPv6

Módulo de Optimización WAN
La optimización WAN tiene como objeto acelerar aplicaciones en redes dispersas a nivel geográfico, y a la vez garantizar una inspección multi-amenaza de todo el tráfico del core de red. La optimización WAN elimina tráfico innecesario y malicioso, optimiza el tráfico legítimo, y reduce la cantidad de ancho de banda requerido para transmitir datos entre aplicaciones y servidores. La mejora de rendimiento, reducción del ancho de banda y consecuente optimización del uso de recursos y requerimientos de infraestructura, permite un mayor control y ahorro de los gastos asociados.
Características:
- Optimización punto a punto
- Optimización bidireccional cliente-servidor
- Caché Web
- Túnel seguro
- Modo transparente

Módulo de Gestión de Conexiones VPN
La tecnología VPN Fortinet proporciona comunicaciones seguras entre múltiples redes y servidores, usando tecnologías SSL e IPsec VPN. Los servicios de FortiGate VPN son el complemento perfecto para completar la inspección y protección de contenido y la prevención de intrusiones en áreas privadas de red. El módulo de gestión de conexiones VPN permite definir políticas de QoS con las que priorizar perfiles de tráfico crítico en comunicaciones que circulen por túneles VPN.

Características:
- IPSec y VPN SSL
- DES, 3DES, AES y Autenticación SHA-1/MD5
- PPTP, L2TP, VPN Pass Through
- SSL Single Sign-on
- Autenticación de Doble Factor

Módulo de Inspección de Tráfico Cifrado-SSL
La inspección del tráfico cifrado-SSL protege de amenazas ocultas a los clientes finales, así como a los servidores web y de aplicación. La inspección SSL intercepta el tráfico cifrado e inspecciona las amenazas antes de enrutarlo a su destino final. Puede ser aplicado a tráfico SSL orientado a cliente, así como, por ejemplo, a los usuarios que quisieran conectarse a un site CRM basado en cloud, o a la totalidad del tráfico entrante de servidores web y aplicaciones.
La funcionalidad de inspección SSL permite forzar el uso de políticas apropiadas sobre contenido web cifrado y proteger a los servidores de amenazas que pueden estar ocultas dentro del flujo de tráfico cifrado.

Características:
- Soporta protocolos: HTTPS, SMTPS, POP3S, IMAPS
- Soporta inspección: Antivirus, Filtrado web, Antispam, Prevención de pérdida de Datos, Terminadores SSL

Módulo de Prevención de Pérdida de Datos (DLP)
DLP usa un sofisticado motor de patrones para identificar y prevenir la transferencia de información sensible fuera del perímetro de nuestra red, incluso cuando las aplicaciones encriptan sus comunicaciones. Además de proteger los datos críticos de las organizaciones, DLP ofrece una traza sobre logs para ayudar al cumplimiento de la política. El usuario puede seleccionar una amplia gama de acciones configurables para registrar, bloquear, y archivar datos, y poner en cuarentena o prohibir usuarios.

Características:
- Control e identificación sobre datos en movimiento
- Base de datos de patrones pre-definidos
- Motor de Búsqueda basado en expresiones regulares
- Inspección de los formatos de fichero más comúnmente utilizados
- Soporta varios idiomas
- DLP basado en flujos

Módulo de Filtrado Web
El filtrado web protege a los servidores, redes e información sensible contra amenazas basadas en web, evitando que los usuarios accedan a sitios web con riesgos de phishing y fuentes de malware. Además, los administradores pueden forzar políticas basándose en categorías que de forma sencilla, evitan que los usuarios accedan a contenido inapropiado evitando que saturen las redes de tráfico no deseado.

Características:
- Filtrado HTTP/HTTPS
- Bloqueo de URL/Palabra clave/Frase
- Bloqueo de Java Applet, Cookies o Active X
- Filtrado de cabeceras de tipo MIME
- Filtrado web basado en flujos

Módulo de Alta Disponibilidad
La solución de Firewall avanzado de Gigas con Fortigate puede ser presentada en modo standalone o HA (alta disponibilidad). Las configuraciones en HA (alta disponibilidad) incrementan el rendimiento y la fiabilidad mediante la creación de clústers de varios nodos de FortiGate. FortiGate HA soporta modos Activo-Activo y Activo-Pasivo para ofrecer la máxima flexibilidad. La funcionalidad de alta disponibilidad está incluida como parte del sistema operativo FortiOS.

Características:
- Activo-Pasivo
- Failover de sesiones (FW y VPN)
- Conexión entre el monitor de estado y el failover
- Detección y Notificación de fallos del dispositivo
- Balanceador de carga

Módulo de control de Registro, Reporte y Monitorización
Los dispositivos de seguridad FortiGate ofrecen extensas posibilidades de registro para el tráfico, sistemas, y funciones de protección de la red. Además, permiten reunir detalles y reportes gráficos de información de log detallada. Los reportes aportan análisis actuales y de histórico de la actividad de la red para ayudar a la identificación de aspectos de seguridad y prevenir usos indebidos o abusos en la red.

Características:
- Almacenamiento de log interno y generación de reportes
- Monitoriazión gráfica en tiempo real e histórica
- Soporte reportes gráficos planificados
- Gráficos en detalle
- Opcional FortiAnalyser Logging (incluido para VDOM)
- Opcional FortiGuard Analysis y Servicio de gestión

Módulo de control de Control de Aplicaciones
El módulo de control de aplicaciones permite reforzar y optimizar la gestión de políticas de seguridad de miles de aplicaciones corriendo en la red, independientemente del puerto o del protocolo usado para la comunicación, así como optimizar el uso de ancho de banda en cada red. El aumento de las aplicaciones basadas en Internet, que hoy en día bombardean las redes, hace que sea esencial el control de la aplicación, dado que la mayoría del tráfico en las aplicaciones parece tráfico normal a los firewalls tradicionales. El módulo de control de aplicaciones de Fortinet ofrece un control granular de aplicaciones junto con la capacidad de establecer políticas de shaping de tráfico e inspección basada en flujos.

Características:
- Identifica y controla más de 1.800 aplicaciones
- Configuración del tráfico (por aplicación)
- Control generalizado de Apps a pesar del puerto o del protocolo
- Incluye Aplicaciones conocidas como:
  - AOL-IM
  - ICQ
  - WinNY
  - Yahoo
  - Gnutella
  - Skype
  - MSN
  - BitTorrent
  - eDonkey
  - KaZaa
  - MySpace
  - Facebook
  - Otras

OPCIONES DE CONFIGURACIÓN

Fortinet ofrece a los administradores una variedad de métodos y asistentes a la hora de configurar los dispositivos en la instalación. Desde un sencillo interfaz web hasta un interfaz por línea de comandos con funcionalidades avanzadas, el sistema ofrece la flexibilidad y sencillez que el cliente necesita.

Características:
- Interfaz de usuario basado en web
- Interfaz de línea de comandos (CLI)

ESPECIFICACIONES TÉCNICAS

ESPECIFICACIONES	GIGAS FG 400	GIGAS FG 600	GIGAS FG 700	GIGAS FG 800
Especificaciones técnicas				
vCPU (Min / Max)	1 / 1	1 / 2	1 / 4	1 / 8
Memoria RAM (Min / Max)	1GB / 2GB	1GB / 4GB	1GB / 6GB	1GB / 12GB
Dominios Virtuales	10 / 10	10 / 25	10 / 50	10 / 250
Políticas de Firewall (System)	20.000 / 40.000	50.000 / 100.000	50.000 / 100.000	50.000 / 100.000
Rendimiento				
Firewall Throughtput (UDP packets)	12 Gbps	15 Gbps	28 Gbps	33 Gbps
IPSec VPN Throughput (AES256+SHA1)	1 Gbps	1.5 Gbps	3 Gbps	5.5 Gbps
IPS Throughput	3.5 Gbps / 1 Gbps	5.5 Gbps / 1.5 Gbps	8 Gbps / 3 Gbps	15.5 Gbps / 6 Gbps
Antivirus Throughput	200 Mbps	300 Mbps	350 Mbps	400 Mbps
Gateway to Gateway IPSec VPN Tunnels (System / VDOM)	2.000	2.000	2.000	40.000
Client-to-Gateway IPSec VPN Tunnels	6.000	12.000	20.000	40.000
Sesiones Concurrentes	1.0 Million	2.6 Million	4.3 Million	8.5 Million
Nuevas Sesiones/Sec	85.000	100.000	125.000	150.000
Usuarios VPN SSL Concurrentes	1.000	2.000	4.500	10.000
VPN - SSL Throughput	800 Mbps	830 Mbps	2 Gbps	4.5 Gbps