Firewalls con IA de la serie eKitEngine USG6000F-S de HUAWEI

Firewalls con IA de la serie eKitEngine USG6000F-S de HUAWEI

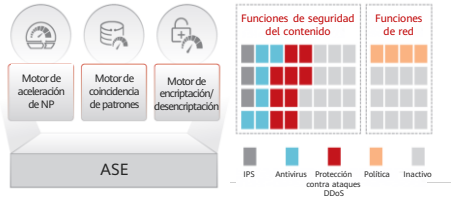
A medida que la digitalización se expande por todo el mundo, las conexiones extensas, el crecimiento explosivo de los datos y el auge de las aplicaciones inteligentes están cambiando profundamente la forma en que vivimos y trabajamos. Los servicios empresariales se están digitalizando y migrando a la nube, lo que promueve la transformación de las redes empresariales al tiempo que plantea mayores desafíos para la seguridad. A medida que aumentan las amenazas, las que son desconocidas cambian constantemente y son muy difíciles de detectar. Debido al incremento en los requerimientos de los usuarios con respecto a los servicios de seguridad, el rendimiento y la latencia se convierten en cuellos de botella. Con una gran cantidad de políticas y logs de seguridad, la gestión de amenazas y las tareas de O&M requieren mucho tiempo. Los firewalls actúan como la “primera puerta” en las fronteras de la red, por lo que son la primera opción para la protección de la seguridad empresarial. Sin embargo, los firewalls tradicionales solo pueden analizar y bloquear amenazas basándose en firmas; por lo tanto, no pueden gestionar eficazmente las amenazas desconocidas. Además, la efectividad de la prevención de amenazas depende de la experiencia profesional del personal de O&M. El enfoque de protección de un solo punto, reactivo y durante el evento no permite defenderse eficazmente de las amenazas desconocidas, y mucho menos de las amenazas ocultas en el tráfico encriptado.

Con nuevas arquitecturas de hardware y software, los firewalls con IA de próxima generación de la serie eKitEngine USG6000F-S de Huawei cuentan con protección inteligente, rendimiento excepcional y O&M simplificado, lo que permite superar eficazmente los desafíos mencionados. Los firewalls con IA de la serie eKitEngine USG6000F-S usan tecnologías de inteligencia para bloquear con precisión las amenazas conocidas y desconocidas a fin de proteger las fronteras. Equipados con múltiples motores de aceleración de seguridad integrados, los firewalls con IA de la serie eKitEngine USG6000F-S aceleran el reenvío de paquetes, la detección de seguridad del contenido y el procesamiento de servicios IPsec. La plataforma de O&M de seguridad implementa la gestión y el O&M unificados de múltiples tipos de productos de seguridad, como firewalls y dispositivos de protección contra ataques DDoS, reduciendo los gastos operativos del O&M de seguridad.

HUAWEI

01 Aspectos destacados del producto

Excelente rendimiento



Valiéndose de arquitecturas nuevas de hardware y software que separan el reenvío del control, los firewalls con IA de la serie eKitEngine USG6000F-S asignan dinámicamente recursos a los módulos de servicio a través del motor de seguridad adaptativo (ASE), maximizando el aprovechamiento de recursos y mejorando el rendimiento general del servicio. Para los servicios principales, la serie eKitEngine USG6000F-S también admite motores de procesadores de red (NP), coincidencia de patrones y encriptación/desencriptación. Estos motores mejoran considerablemente el reenvío de paquetes cortos, reducen la latencia de reenvío y mejoran la identificación de aplicaciones, la detección de prevención de intrusiones y el rendimiento del servicio IPsec.

Protección inteligente

- ✓ Firmas: familias de archivos maliciosos = **1: N**
- ✓ Alta velocidad de detección **comparable a la de la detección basada en firmas de virus**
- ✓ Capacidad de detectar **amenazas desconocidas**

Los firewalls con IA de la serie eKitEngine USG6000F-S cuentan con funciones de seguridad de contenido, como identificación de aplicaciones, IPS, antivirus y filtrado de URL para proteger servidores de intranet y usuarios contra las amenazas. La serie eKitEngine USG6000F-S también puede detectar amenazas desconocidas mediante la interoperación con el entorno de pruebas aislado.

Las firmas de IPS tradicionales se producen manualmente, ocasionando una baja productividad. Además, la precisión de las firmas depende en gran medida de la experiencia de los expertos. Huawei produce de manera innovadora firmas de IPS en la nube inteligente mediante tecnologías de inteligencia y la experiencia de expertos. Esto multiplica la productividad de las firmas por 30 en comparación con la producción manual, reduce los errores causados por el análisis manual y mejora continuamente la precisión de la detección de intrusiones.

El motor integrado de detección de antivirus basado en contenidos (CDE), que cuenta con tecnologías de inteligencia, puede detectar amenazas desconocidas y proporcionar un análisis de datos profundo. Con estas capacidades, el firewall potenciado con CDE puede obtener información sobre las amenazas y detectar rápidamente archivos maliciosos, mejorando eficazmente la tasa de detección de amenazas.

La serie eKitEngine USG6000F-S puede detectar y evitar la propagación del software malicioso y los ataques a la red (gusanos, virus, troyanos, spyware, propagación de software malicioso y botnet, DoS/DDoS, inyección de SQL, secuencias de órdenes en sitios cruzados y ransomware).

O&M simplificado

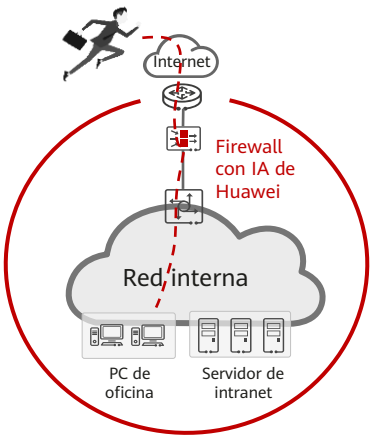
Los firewalls con IA de la serie eKitEngine USG6000F-S cuentan con una interfaz de usuario web totalmente nueva que permite visualizar de forma intuitiva las amenazas y muestra información clave, como el estado del dispositivo, las alarmas, el tráfico y los eventos de amenazas. Con el análisis multidimensional de datos, la interfaz de usuario web ofrece una experiencia óptima para el usuario, así como mejor usabilidad y O&M simplificado.

La serie eKitEngine USG6000F-S puede gestionarse de forma centralizada mediante la plataforma de gestión de seguridad SecoManager, lo que permite pasar de la protección en un solo punto a la protección de red colaborativa. SecoManager cuenta con capacidades de adecuación de políticas y O&M inteligente. También puede gestionar otros productos de seguridad, como dispositivos de protección contra ataques DDoS, para eliminar rápidamente las amenazas a la red y mejorar la eficacia de la gestión de la seguridad.

La serie eKitEngine USG6000F-S también puede ser gestionada por el NCE-Campus, que también permite gestionar switches y dispositivos AR y POL, e incluso dispositivos de terceros.

Amplia gama de funciones de red

La serie eKitEngine USG6000F-S de Huawei también ofrece diversas funciones de red, como VPN, IPv6 y selección inteligente de uplink.



- Proporciona diversas funciones de VPN, como VPN sobre IPsec y VPN SSL, y admite múltiples algoritmos de encriptación, como DES, 3DES, AES y SHA, garantizando una transmisión de datos segura y confiable.
- Permite una transición segura y completa a la red IPv6, así como control de políticas, protección de seguridad y visualización del servicio. Esto ayuda a Gobiernos, medios de comunicación, operadores, compañías de Internet y entidades financieras a migrar a IPv6.
- Permite la selección inteligente tanto dinámica como estática de uplink entre múltiples enlaces de salida, escoge la interfaz de salida según el ancho de banda, la ponderación o la prioridad del enlace especificado, reenvía el tráfico a cada enlace según el modo de selección de uplink especificado, y ajusta dinámicamente el resultado de la selección de enlaces en tiempo real para maximizar el aprovechamiento de los enlaces y mejorar la experiencia del usuario.

02 Implementación

Protección de fronteras en centros de datos pequeños

- Los firewalls se despliegan en las salidas de los centros de datos, y las funciones y los recursos del sistema se pueden virtualizar. El firewall tiene múltiples tipos de interfaces, como 10GE y GE. Los servicios se pueden expandir con flexibilidad sin tarjetas de interfaz adicionales.
- La capacidad de prevención de intrusiones bloquea eficazmente diversos ataques maliciosos y ofrece una protección diferenciada según los requerimientos del entorno virtual para garantizar la seguridad de los datos.
- Se pueden establecer túneles VPN entre los firewalls y los empleados móviles, así como entre los firewalls y las sucursales, para garantizar que el acceso remoto y el trabajo móvil sean seguros y rentables.

Protección de fronteras empresariales

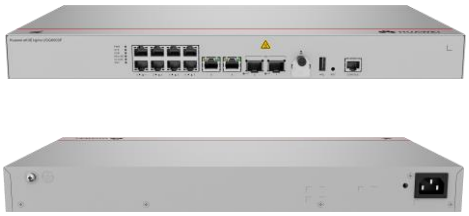
- Los firewalls se despliegan en la frontera de la red. La sonda de tráfico integrada puede extraer paquetes de tráfico encriptado para monitorear las amenazas en tiempo real.
- Las funciones de control de políticas y filtrado de datos de los firewalls monitorean las aplicaciones de redes sociales para evitar la violación de datos y proteger las redes empresariales.

03 Aspecto del producto

- **Amplias capacidades de acceso**: Ethernet, RU 5G

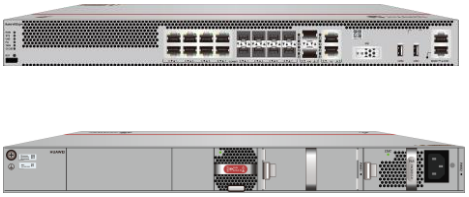
- **Figura 3-1**

eKitEngine USG6000F-S125



- **Figura 3-2**

eKitEngine USG6000F-S150



- **Figura 3-3**

eKitEngine USG6000F-S200

04 Características del software

Característica	Descripción
Protección integrada	Integra funciones de firewall, VPN, prevención de intrusiones, antivirus, gestión de ancho de banda, protección contra ataques DDoS y filtrado de URL, y ofrece una vista global de la configuración, así como gestión integrada de políticas.
Identificación y control de aplicaciones	Identificación de aplicaciones basada en firmas, correlaciones y comportamientos en lugar de puertos; más de 6,000 aplicaciones preestablecidas, que se pueden subclasificar; compatibilidad con aplicaciones definidas por el usuario; más de 50 categorías y más de 20 etiquetas de riesgo para el control de acceso basado en categorías y etiquetas; actualización automática de la base de datos de firmas de identificación de aplicaciones
Gestión de políticas de seguridad	Admite la gestión y el control del tráfico en función del ID de VLAN, las 5 tuplas, la zona de seguridad, la región, la aplicación y el intervalo de tiempo, e implementa la inspección integrada de seguridad del contenido. Proporciona plantillas predefinidas para escenarios comunes de protección contra ataques para facilitar la implementación de políticas de seguridad. Admite la interoperación con software de gestión de políticas de terceros (FireMon y AlgoSec) para facilitar las tareas de O&M de seguridad.
Gestión de ancho de banda	Gestiona el ancho de banda por IP en función de la identificación de las aplicaciones de servicio para garantizar la experiencia de red de los servicios y usuarios clave. La gestión y el control se pueden implementar limitando el ancho de banda máximo, garantizando el ancho de banda mínimo y cambiando la prioridad de reenvío de las aplicaciones.
Prevención de intrusiones	Obtiene la información más reciente de las amenazas de manera oportuna, y detecta y previene con precisión las vulnerabilidades de seguridad; cubre decenas de miles de vulnerabilidades de CVE; evita la explotación de vulnerabilidades de seguridad (como las de los sistemas operativos Windows y Unix/Linux, bases de datos, Apache, IIS y Tomcat, así como middleware), los ataques web (como la inyección de SQL, XSS y RCE), las botnets, el control remoto y los troyanos; admite la detección de descifrado por fuerza bruta según el comportamiento del usuario; proporciona más de 25,000 firmas predefinidas y admite las firmas definidas por el usuario y la actualización automática de la base de datos de firmas; admite la recopilación forense de ataques, la obtención de paquetes de flujo completo (incluida la información de handshake de tres vías) y la visualización de fragmentos de ataques para facilitar las tareas de O&M; admite la extracción de campos X-Forwarded-For (XFF).
Antivirus	Detecta el software malicioso en archivos transmitidos a través de protocolos como HTTP, FTP, SMTP, POP3, IMAP4, NFS y SMB; detecta troyanos, gusanos, spyware, explotación de vulnerabilidades de seguridad, software de publicidad, herramientas de hackers, Rootkit, puertas traseras, software no autorizado, programas de botnet, ransomware, software de fraude electrónico, software de criptojacking y programas web shell; admite la detección de virus en archivos de Office, archivos ejecutables (Windows/Linux/macOS), archivos de script, archivos flash, archivos PDF, archivos RTF, páginas web e imágenes; admite la recopilación forense de ataques; admite la inspección de archivos de hasta 100 niveles anidados de compresión en múltiples formatos de compresión, como tar, gzip, zip, rar y 7z; y admite múltiples acciones, como alertas, bloqueos, expansión de listas de amenazas conocidas y eliminación de adjuntos.
Prevención avanzada de software malicioso	El motor antivirus heurístico utiliza tecnologías de detección como IA, análisis semántico y emulador, junto con información sobre amenazas y reputación, para detectar software malicioso empaquetado, transformación de scripts y software malicioso integrado en documentos compuestos. Puede detectar miles de millones de variantes de software malicioso y admite la actualización automática de la base de datos de firmas. Además, puede enviar archivos sospechosos al entorno de prueba local o en la nube para inspeccionarlos en profundidad y detectar el software malicioso de día cero.
Seguridad web	La base de datos de categorías de URL en la nube incluye 560 millones de URL correspondientes a más de 130 categorías, como noticias, juegos, apuestas, drogas y páginas web maliciosas. Las URL cubren más de 100 idiomas, y las categorías clave de las URL cubren más de 20 idiomas. Los servidores de consulta de categorías de URL se despliegan en múltiples países/regiones para proporcionar servicios de alta velocidad y baja latencia. Se admiten las listas de confianza y listas de bloqueo de URL/hosts definidas por el usuario. El tráfico HTTPS se puede filtrar sin desencriptarlo.

Característica	Descripción
Seguridad web	El tráfico TLS/SSL se puede desencriptar antes de filtrarlo. El tráfico HTTP/2 y QUIC se puede filtrar, y las categorías de URL se pueden importar por lotes. Admite las búsquedas seguras en cinco motores de búsqueda principales: YouTube, Bing, Google, Yahoo y Yandex, con filtrado obligatorio de contenido ilegal o inapropiado en los resultados de las búsquedas. El acceso a URL se puede controlar en función de los usuarios/grupos de usuarios, los períodos y las zonas de seguridad para gestionar con precisión los comportamientos en línea de los usuarios.
Seguridad de DNS	Sobre la base de una gran cantidad de información de amenazas, se usan tecnologías como la IA y los gráficos de conocimientos para detectar solicitudes de DNS maliciosas, incluyendo nombres de dominio de C&C, nombres de dominio generados por DGA, sitios comprometidos y nombres de dominio maliciosos, como nombres de dominios de criptojacking, ransomware y fraude electrónico. La base de datos local de nombres de dominio maliciosos admite un máximo de 2 millones de nombres de dominio maliciosos. También se admiten el filtrado basado en categorías de DNS, la búsqueda segura de DNS y el redireccionamiento de DNS (sinkholing).
Software contra botnets y spyware	Admite la detección y prevención de virus y software malicioso avanzado, como botnets, troyanos, gusanos, herramientas de control remoto y spyware, y evita la descarga de software malicioso; detecta rápidamente el tráfico malicioso, como el C&C basado en firmas, direcciones IP e información de reputación de dominios; muestra los roles de los integrantes de la comunicación en los logs de ataques de botnets.
Información de amenazas	El Centro de Seguridad Inteligente de Huawei adopta múltiples algoritmos de IA y análisis de expertos para generar a diario una gran cantidad de información de amenazas de direcciones IP, nombres de dominio, URL y archivos. La información de amenazas se sincroniza automáticamente con los dispositivos para la detección de amenazas y el bloqueo rápido de los ataques emergentes. Además, puede interconectarse con fuentes externas de información de amenazas para enriquecer las reglas de inspección.
Protección contra ataques DDoS	Utiliza tecnologías como la detección de direcciones IP de origen, la detección de huellas digitales y la limitación dinámica del tráfico para ofrecer protección contra más de 10 tipos comunes de ataques DDoS y más de 20 tipos de ataques de un solo paquete, como los ataques de saturación de SYN, UDP, ICMP, HTTP, HTTPS, DNS y SIP, y admite el aprendizaje de la línea de base del tráfico y el filtrado según la reputación IP (no se admite en el USG6000F-S125).
Filtrado de correos	Admite el filtrado de direcciones de correo (incluyendo las direcciones del remitente y del destinatario) y la limitación de la velocidad de envío de correos SMTP.
DLP	Admite la identificación de más de 100 tipos de archivos reales, extensiones de nombres de archivos definidas por el usuario, y el control de cargas/descargas según el tipo de archivo; admite el filtrado de palabras clave para documentos de Office, páginas web, códigos y archivos TXT; admite palabras clave definidas por el usuario, expresiones regulares y configuración de ponderación.
Capacidad de O&M	Admite telemetría para leer automáticamente la información del hardware, incluyendo ventiladores, módulos de alimentación, módulos ópticos, puertos Ethernet, sensores de temperatura y controladores, y envía al recolector las estadísticas de tráfico de interfaces, uso de la CPU y uso de la memoria.
PPPoE	Funciona como un cliente PPPoE para proporcionar servicios de acceso a Internet, incluyendo la autenticación y autorización de usuarios, así como la asignación dinámica de direcciones IP.
Verificación de cumplimiento de seguridad	Admite la verificación de la versión del sistema operativo, la verificación de parches del sistema operativo, la verificación del software antivirus, la verificación del firewall, la verificación de procesos en ejecución, la verificación de seguridad de los archivos, la verificación de registros, la verificación de puertos, la protección contra capturas de pantalla y la prevención de conexiones anidadas remotas de escritorio.

Característica	Descripción
Auditoría de comportamientos	Audita y regula los comportamientos en línea comunes de los usuarios, incluyendo operaciones FTP (cargas, descargas y comandos), operaciones HTTP (publicación, búsqueda y navegación), DNS, Telnet, SNMP, y las operaciones de envío y recepción de correos electrónicos.
Selección inteligente de uplink	Admite PBR de servicios específicos y escoge de forma inteligente el enlace óptimo según múltiples tipos de criterios de balanceo de carga (como la relación del ancho de banda y el estado de funcionamiento del enlace) en escenarios de múltiples ISP.
Encriptación de VPN	Admite diversas funciones altamente confiables de VPN, como VPN sobre IPsec, VPN SSL y GRE, así como múltiples algoritmos de encriptación, como DES, 3DES, AES, SHA, SM2, SM3 y SM4.
Inspección de tráfico encriptado con SSL	Detecta amenazas ocultas en el tráfico encriptado con TLS/SSL y ofrece protección contra ellas, protege la capa de aplicaciones, que incluye la prevención de intrusiones, los antivirus, el filtrado de datos y de URL en el tráfico TLS/SSL desencriptado, y admite la lista de confianza de categorías de URL.
Descarga de SSL	Reemplaza el servidor para implementar la encriptación y desencriptación de SSL, lo que reduce la carga del servidor y permite implementar el balanceo de carga del tráfico HTTP.
Reportes diversificados	Proporciona reportes visualizados y multidimensionales según la dirección IP, la aplicación, la fecha/hora, el tráfico o la amenaza.
Virtualización de la seguridad	Admite la virtualización de múltiples tipos de servicios de seguridad, incluyendo servicios de firewall, prevención de intrusiones, antivirus y VPN; permite a los usuarios realizar una gestión personalizada por separado en el mismo dispositivo físico.
Enrutamiento	Admite múltiples tipos de protocolos de enrutamiento IPv4/IPv6, como RIP, OSPF, BGP, IS-IS, RIPng, OSPFv3, BGP4+ e IS-IS IPv6.
Multicast de IP	Admite protocolos multicast IPv4 de capa 3, como IGMP, MSDP y PIM, y proporciona servicios punto a multipunto para reducir el consumo de ancho de banda.
Balanceo de carga del servidor	Admite el balanceo de carga de servidores de capa 4/7 e IPv6, así como múltiples métodos de persistencia de sesiones, como la persistencia de sesiones basada en direcciones IP de origen y en cookies HTTP; admite la descarga y encriptación de SSL; combina servicios y políticas de seguridad para mejorar la seguridad del servicio; admite la comprobación de estado basada en múltiples protocolos, como TCP, RADIUS, DNS y HTTP, para detectar rápidamente los cambios de estado del servidor.
Despliegue y confiabilidad	Admite modos de funcionamiento transparente (capa 2), de enrutamiento (capa 3) e híbridos, así como alta disponibilidad (HA), incluyendo los modos activo/activo y activo/standby.
Centro de seguridad	El módulo integrado de identificación de activos puede identificar activos de Windows, Linux, Android e iOS, así como cámaras; puede analizar correlaciones en logs de amenazas y activos, y mostrar los resultados de la evaluación de riesgos de los activos y todo el proceso de eliminación (kill chain).
SRv6	Admite IS-IS para SRv6, BGP para SRv6, SRv6 BE, política de SRv6 TE, protección de punto medio de SRv6, capacidad para evitar microbucles de SRv6, OAM de SRv6, compresión de SRH de SRv6, TI-LFA FRR de SRv6 y L3VPN de EVPN.
SD-WAN segura	Ofrece una solución SD-WAN integrada y segura para enlaces de Internet empresariales de bajo costo. Admite el aprovisionamiento sin intervención (ZTP) a través del correo electrónico para completar el aprovisionamiento del dispositivo con facilidad en cuestión de minutos. Admite la corrección de errores hacia adelante (FEC) para evitar la visualización pixelada y el almacenamiento en búfer a una tasa de pérdida de paquetes del 30 %; admite la conmutación de enlaces en tiempo real según la calidad del enlace para garantizar la experiencia de las aplicaciones clave. Admite el enrutamiento de múltiples enlaces y redes flexibles de CPE duales para garantizar que no se interrumpan las conexiones de los servicios del sitio; admite la encriptación IPsec de extremo a extremo para garantizar la transmisión segura del servicio.
Autenticación de usuarios	Admite múltiples modos de autenticación para los usuarios de acceso a Internet, incluyendo la autenticación local vía portal y el inicio de sesión único (SSO). En la autenticación local vía portal, se puede mostrar una página de portal integrada del dispositivo a los usuarios, y la cuenta y la contraseña que el usuario ingresa en la página del portal se pueden enviar a la base de datos local o al servidor de autenticación RADIUS, HWTACACS, AD o LDAP para su autenticación. El SSO incluye SSO de RADIUS y SSO de Agile Controller (NCE-Campus).

05 Especificaciones

• Rendimiento y capacidad del sistema

Modelo	USG6000F-S125	USG6000F-S150	USG6000F-S200
Cantidad máxima de usuarios recomendada	600	1,000	2,500
Throughput [1] del firewall IPv4 (1,518/512/64 bytes, UDP)	8/8/3.6 Gbps	12/12/4 Gbps	16/16/5 Gbps
Throughput [1] del firewall IPv6 (1,518/512/84 bytes, UDP)	8/8/3.6 Gbps	12/12/4 Gbps	16/16/5 Gbps
Throughput seguro de EVPN de SD-WAN (1,400/512 bytes, UDP) [8]	5/5 Gbps	9/6.6 Gbps	10/6.8 Gbps
Máximo de túneles seguros de EVPN de SD-WAN	200	200	200
Latencia del firewall (64 bytes, UDP)	18 µs	18 µs	18 µs
Latencia del firewall (64 bytes, UDP) [7]	7 µs	7 µs	7 µs
Máximo de sesiones simultáneas (HTTP1.1) [1]	1,000,000	4,000,000	4,000,000
Máximo de sesiones nuevas/segundo (HTTP1.1) [1]	50,000	80,000	120,000
Throughput [2] de FW + SA*	2 Gbps	2.8 Gbps	4.5 Gbps
Throughput de NGFW (HTTP 100K) [3]	1.7 Gbps	2.1 Gbps	3 Gbps
Throughput de NGFW (combinación empresarial) [4]	1.2 Gbps	1.3 Gbps	2 Gbps
Throughput de protección contra amenazas (FW + SA + IPS + AV, HTTP 100K) [9]	1.4 Gbps	1.8 Gbps	2.5 Gbps
Throughput de protección contra amenazas (combinación empresarial) [5]	1 Gbps	1.2 Gbps	1.8 Gbps
Throughput de VPN sobre IPsec (AES-256 + SHA256; 1,420 bytes) [1]	3.7 Gbps	3.5 Gbps	5.6 Gbps
Máximo de túneles VPN sobre IPsec	2,000	4,000	4,000
Throughput [6] de VPN SSL	300 Mbps	500 Mbps	750 Mbps
Usuarios de VPN SSL simultáneos* (valor predeterminado/máximo)	100/1,000	100/1,600	100/2,000
Políticas de seguridad (máximo)	3,000	15,000	15,000
Firewalls virtuales	20	100	100
Filtrado de URL: Categorías	>130		
Filtrado de URL: URL	Base de datos de más de 560 millones de URL en la nube		
Actualizaciones automatizadas de firmas de IPS	Sí, un centro de seguridad de Huawei líder en la industria (https://isecurity.huawei.com/security/service/ips)		
Ecosistema externo de código abierto	Interfaces Open API y NETCONF para la integración con productos de terceros y software de gestión de terceros que usan SNMP, SSH o Syslog		
Máximo de redes VLAN	4,094		
Máximo de interfaces VLANIF	4,094		

1. El rendimiento se somete a prueba bajo condiciones ideales según las RFC 2544 y RFC 3511. El resultado real puede variar según los entornos de despliegue.
2. Los indicadores de rendimiento de SA se miden usando archivos HTTP de 100 kB.
3. El throughput de NGFW se mide con el firewall, SA e IPS habilitados; el rendimiento se mide usando archivos HTTP de 100 kB.
4. El throughput de NGFW se mide con el firewall, SA e IPS habilitados; el rendimiento se mide utilizando el modelo de tráfico combinado empresarial.
5. El throughput de protección contra amenazas se mide con el firewall, SA, IPS y antivirus habilitados; el rendimiento se mide usando el modelo de tráfico combinado empresarial.
6. El throughput de VPN SSL se mide usando TLS v1.2 con AES128-SHA.
7. Los datos se someten a prueba en modo de par de interfaces.
8. El túnel SD-WAN se encapsula con GRE sobre IPsec.
9. El throughput de protección contra amenazas se mide con el firewall, SA, IPS y antivirus habilitados; los indicadores de rendimiento se miden usando archivos HTTP de 100 kB.

*SA: reconocimiento de servicios

06 Especificaciones de hardware

Modelo	USG6000F-S125	USG6000F-S150	USG6000F-S200
Altura del chasis	1 U (mitad)	1 U	
Dimensiones (altura × ancho × profundidad) en mm	43.6 × 442 × 220	43.6 × 442 × 420	
Puertos fijos	2 puertos 10GE (SFP+) + 10 puertos GE	2 puertos 10GE (SFP+) + 8 puertos GE Combo + 2 puertos GE	2 puertos 10GE (SFP+) + 8 puertos GE Combo + 16 puertos GE
Puertos USB	1 puerto USB 3.0	2 puertos USB 3.0	1 puerto USB 3.0
Peso	2.32 kg	5.46 kg	5.816 kg
Almacenamiento externo	Opcional, tarjeta microSD de 64 GB disponible para la compra	Opcional, se admite SSD M.2, 64 GB/240 GB/960 GB	
Fuente de alimentación (CA)	100 V-240 V, 50 Hz/60 Hz		
Potencia máxima	27.4 W	49.5 W	53.2 W
Módulo de alimentación	Un solo módulo de alimentación de CA	Dos módulos de alimentación de CA	
Entorno de funcionamiento (temperatura/humedad)	Temperatura: de 0 °C a +45 °C Humedad: del 5 % al 95 %, sin condensación		
Entorno no relacionado con el funcionamiento	Temperatura: de -40 °C a +70 °C Humedad: del 5 % al 95 %, sin condensación		
Tipo de instalación	Montaje en rack		

07 Información para los pedidos

- **Nota:**

  - Algunas partes de esta tabla especifican las estrategias de ventas correspondientes a diferentes regiones. Para obtener más información, comuníquese con el representante de Huawei.

Producto	Modelo	Descripción
USG6000F-S125	USG6000F-S125-AC	Host de CA del USG6000F-S125: 2 puertos 10GE (SFP+) + 10 puertos GE, 1 módulo de alimentación de CA
USG6000F-S150	USG6000F-S150-AC	Host de CA del USG6000F-S150: 2 puertos 10GE (SFP+) + 8 puertos GE Combo + 2 puertos GE, 1 módulo de alimentación de CA
USG6000F-S200	USG6000F-S200-AC	Host de CA del USG6000F-S150: 2 puertos 10GE (SFP+) + 8 puertos GE Combo + 16 puertos GE, 1 módulo de alimentación de CA
Licencia de las funciones		
VPN SSL	LIC-USG6KF-SSLVPN-20	Cant. máx. de usuarios simultáneos de VPN SSL: 20
	LIC-USG6KF-SSLVPN-50	Cant. máx. de usuarios simultáneos de VPN SSL: 50
Licencia de NGFW		
Servicios de protección contra amenazas (IPS + AV + gestión de comportamientos en línea + información de amenazas) (1/3 años)	LIC-USG6000F-S125-TP-OVS	Suscripción a protección contra amenazas por año (aplicable al USG6000F-S125 fuera de China continental)
	LIC-USG6000F-S150-TP-OVS	Suscripción a protección contra amenazas por año (aplicable al USG6000F-S150 fuera de China continental)
	LIC-USG6000F-S200-TP-OVS	Suscripción a protección contra amenazas por año (aplicable al USG6000F-S200 fuera de China continental)
Servicios de protección avanzada contra amenazas (IPS + AV + filtrado de URL + gestión de comportamientos en línea + información de amenazas) (1/3 años)	LIC-USG6000F-S125-ATP-OVS	Suscripción a protección avanzada contra amenazas por año (aplicable al USG6000F-S125 fuera de China continental)
	LIC-USG6000F-S150-ATP-OVS	Suscripción a protección avanzada contra amenazas por año (aplicable al USG6000F-S150 fuera de China continental)
	LIC-USG6000F-S200-ATP-OVS	Suscripción a protección avanzada contra amenazas por año (aplicable al USG6000F-S200 fuera de China continental)
Servicios de protección empresarial contra amenazas (IPS + AV + filtrado de URL + seguridad de control industrial + gestión de comportamientos en línea + información de amenazas) (1/3 años)	LIC-USG6000F-S150-ESP-OVS	Suscripción a protección empresarial contra amenazas por año (aplicable al USG6000F-S150 fuera de China continental)
	LIC-USG6000F-S200-ESP-OVS	Suscripción a protección empresarial contra amenazas por año (aplicable al USG6000F-S200 fuera de China continental)