HUAWEI eKitEngine USG6000F-S Series AI Firewalls

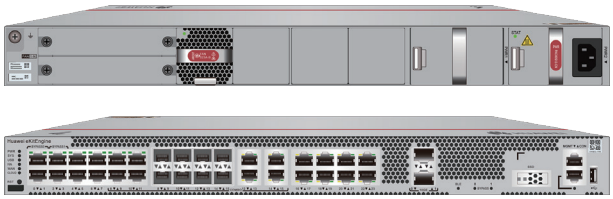
As digitalization is sweeping the world, extensive connections, explosive growth of data, and booming intelligent applications are profoundly changing the way we live and work. Enterprise services are going digital and moving to the cloud, which promotes the transformation of enterprise networks while bringing greater challenges to network security. As threats increase, unknown threats are ever-changing and highly covert. As users' requirements for security services increase, performance and latency become bottlenecks. With mass numbers of security policies and logs, threat handling and O&M are extremely time-consuming. As the "first gate" on network borders, firewalls are the first choice for enterprise security protection. However, traditional firewalls can only analyze and block threats based on signatures and therefore are unable to effectively handle unknown threats. In addition, the effectiveness of threats depends on the professional experience of O&M personnel. The single-point, reactive, and in-event defense method cannot effectively defend against unknown threat attacks, let alone threats hidden in encrypted traffic.

With new hardware and software architectures, Huawei eKitEngine USG6000F-S series, in either desktop or 1 U models, are next-generation AI firewalls that feature intelligent defense, outstanding performance, and simplified O&M, effectively addressing the preceding challenges. The USG6000F-S series uses intelligence technologies to enable border defense to accurately block known and unknown threats. Equipped with multiple built-in security-dedicated acceleration engines, the USG6000F-S series firewalls support enhanced forwarding, content security detection, and IPsec service processing acceleration. The security O&M platform implements unified management and O&M of multiple types of security products, such as firewalls, anti-DDoS devices, reducing security O&M OPEX. In addition, the USG6000F-S-DL series support the LTE function, which ,can be used to implement flexible, efficient, and fast network deployment in remote areas or mobile office scenarios.

HUAWEI

Product Appearance

eKitEngine USG6000F-S125

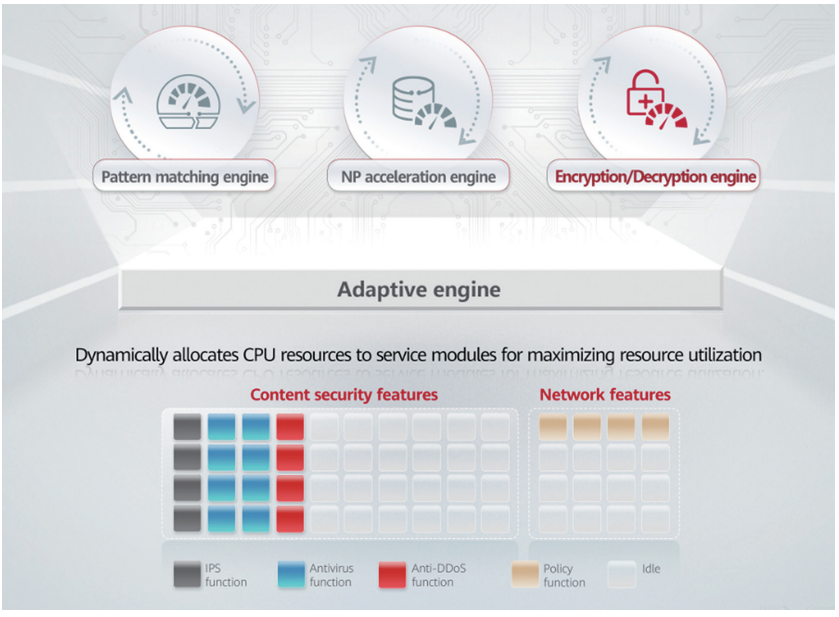


eKitEngine USG6000F-S200

Product Highlights

Excellent performance

By leveraging fresh-new hardware and software architectures, eKitEngine USG6000F-S series AI firewalls dynamically allocate resources to service modules through the adaptive security engine (ASE), maximizing resource utilization and improving overall service performance. For core services, the HiSecEngine USG6000F-S series also supports network processor (NP), pattern matching, and encryption/decryption engines. These engines greatly improve short-packet forwarding, reduce the forwarding latency, and enhance application identification, intrusion prevention detection, and IPsec service performance.

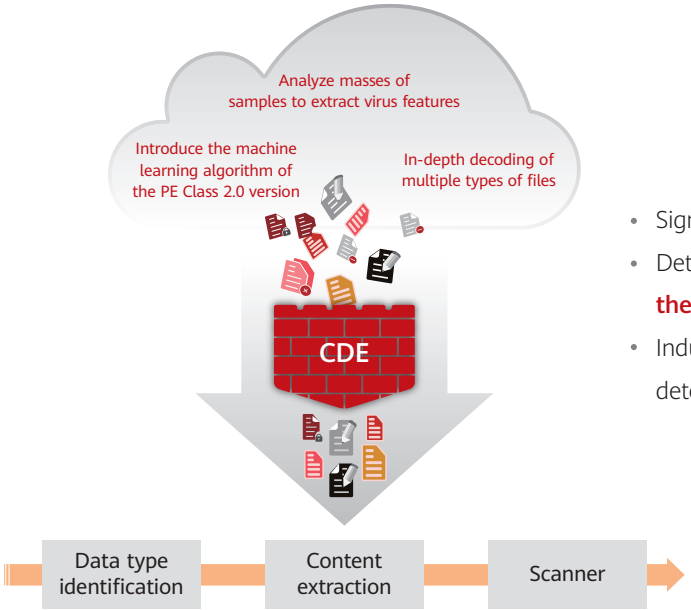


Intelligent defense

eKitEngine USG6000F-S series AI firewalls provide content security functions, such as application identification, IPS, antivirus, and URL filtering to protect intranet servers and users against threats.

Traditional IPS signatures are manually produced through analysis, resulting in low productivity. Also, the accuracy of the signatures depends heavily on expert experience. Huawei innovatively enables the IPS signature production on the intelligent cloud by adopting intelligence technologies and utilizing expert experience. Such an intelligent mode helps increase the signature productivity by 30 times compared with manual production, reduce errors caused by manual analysis, and continuously improve the accuracy of intrusion detection.

The built-in antivirus content-based detection engine (CDE) powered by intelligence technologies can detect unknown threats and provide in-depth data analysis. With these capabilities, the CDE- boosted firewall is able to gain insight into threat activities and quickly detect malicious files, effectively improving the threat detection rate.



- Signature: Malicious file family = **1:N**
- Detection speeds are **equivalent to the signature detection performance**
- Industry-leading **unknown threat** detection capabilities

Simplified O&M

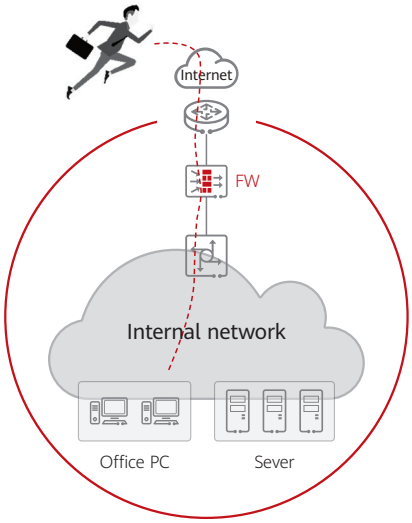
The eKitEngine USG6000F-S series provides a brand-new web UI, which intuitively visualizes threats as well as displays key information such as device status, alarms, traffic, and threat events. With multi-dimensional data drilling, the web UI offers optimal user experience, enhanced usability, and simplified O&M.

The eKitEngine USG6000F-S series firewalls can be centrally managed by the security management platform SecoManager, implementing a shift from single-point defense to collaborative network protection. The SecoManager provides policy tuning and intelligent O&M capabilities. It can also manage security products, such as anti-DDoS devices to quickly eliminate network threats and improve security handling effectiveness.

A wide range of network features

Huawei eKitEngine USG6000F-S series also provides various network features such as VPN, IPv6, and intelligent traffic steering.

- Provides various VPN features such as IPsec VPN and SSL VPN, and supports multiple encryption algorithms, such as DES, 3DES, AES, and SHA, ensuring secure and reliable data transmission.



- Provides secure and rich IPv6 network switchover, policy control, security protection, and service visualization capabilities, helping government, media, carrier, Internet, and finance sectors implement IPv6 reconstruction.
- Provides dynamic and static intelligent traffic steering based on multi-egress links, **selects the outbound interface** based on the specified link bandwidth, weight, or priority, forwards traffic to each link based on the specified traffic steering mode, and dynamically tunes the link selection result in real time to maximize the usage of link resources and improve user experience.

Software Features

Feature	Description
Integrated protection	Integrates firewall, VPN, intrusion prevention, antivirus, bandwidth management, Anti-DDoS, URL filtering; provides a global configuration view; manages policies in a unified manner.
Application identification and control	Identifies over 6,000 applications and supports the access control granularity down to application functions; combines application identification with intrusion detection, antivirus, and data filtering, improving detection performance and accuracy.

Feature	Description
Intrusion prevention and web protection	Obtains the latest threat information in a timely manner for accurate detection and defense against vulnerability-based attacks. Supports coverage of tens of thousands of Common Vulnerabilities and Exposures (CVE). Detects malicious traffic, such as vulnerability attack traffic, web attack traffic (such as SQL injection and cross-site scripting attacks), botnets, remote control, and Trojan horses, and supports brute-force attack detection. Supports 25,000+ IPS signatures, and supports user-defined signatures. The default IPS blocking rate is up to 85%. Supports brute-force cracking detection based on user behaviors, and user-defined statistical periods.
Anti-botnet	Supports detecting Botnet traffic by using the intrusion prevention function.
Antivirus	Supports intelligent, heuristic antivirus engine that can detect hundreds of millions of virus variants. And supports the detection of files compressed in 100 layers.
Bandwidth management	Manages per-user and per-IP bandwidth based on service application identification, ensuring the network experience of key services and users. The management and control can be implemented by limiting the maximum bandwidth, guaranteeing the minimum bandwidth, and changing the application forwarding priority.
URL filtering	Provides a URL category database with over 560 million URLs and accelerates access to specific categories of websites, improving access experience of high-priority websites. Supports DNS filtering, in which accessed web pages are filtered based on domain names. Supports the anti-phishing URL filter.
Intelligent uplink selection	Supports service-specific PBR and intelligent uplink selection based on multiple load balancing algorithms (for example, based on bandwidth ratio and link health status) in multi-egress scenarios.
VPN encryption	Supports multiple highly available VPN features, such as IPsec VPN, SSL VPN and GRE.
SSL-encrypted traffic detection	Detects and defends against threats in SSL-encrypted traffic using application-layer protection methods, such as intrusion prevention, antivirus, data filtering, and URL filtering.
Security virtualization	Supports virtualization of multiple types of security services, including firewall, intrusion prevention, antivirus, and VPN. Users can separately conduct personal management on the same physical device.
Security policy management	Manages and controls traffic based on VLAN IDs, quintuples, security zones, regions, applications, URL categories, and time ranges, and implements integrated content security detection. Provides predefined common-scenario defense templates to facilitate security policy deployment.
Routing	Supports multiple types of routing protocols and features, such as RIP, OSPF, BGP, IS-IS, RIPng, OSPFv3, BGP4+, and IPv6 IS-IS.
Deployment and reliability	Supports transparent, routing, and hybrid working modes and high availability (HA), including the Active/Active and Active/Standby modes.
Server load balancing	Supports IPv6, L4/L7 server load balancing, and multiple session persistence methods based on source IP addresses and HTTP cookies; supports SSL offloading and encryption; supports combination of services and security policies for effective service security enhancement; supports health check based on multiple protocols, such as TCP, RADIUS, DNS, and HTTP, to detect server status changes in a timely manner.
Asset management	Provides asset-based threat visualization, which supports associating IPS and Antivirus threat logs with user assets and displaying asset risk assessment results.

Specifications

System Performance and Capacity

Model	USG6000F-S125	USG6000F-S200
IPv4 Firewall Throughput[1] (1518/512/64-byte, UDP)	2.5/2.5/2.5 Gbit/s	10/10/5 Gbit/s
IPv6 Firewall Throughput[1] (1518/512/84-byte, UDP)	2.5/2.5/2.5 Gbit/s	10/10/5 Gbit/s
Maximum number of concurrent connections (HTTP1.1)	1000,000	4000,000
Number of new connections per second (HTTP1.1)	30,000	120,000
FW + SA Throughput (HTTP 100 KB pages)	1.5 Gbit/s	4.5 Gbit/s
FW + SA + IPS Throughput (HTTP 100 KB pages)	1.2 Gbit/s	3 Gbit/s
FW + SA + IPS + Antivirus Throughput (HTTP 100 KB page)	1 Gbit/s	2.5 Gbit/s
Throughput of FW + SA + IPS + Antivirus (Realworld)	600 Mbit/s	1.8 Gbit/s
IPSec Throughput[1] (AES-256 + SHA256, 1420-byte)	2 Gbps	5.6 Gbps
Number of IPsec VPN tunnels	2000	4000
SSL VPN Throughput	300 Mbit/s	700 Mbit/s
Number of concurrent SSL VPN users (Default/Maximum)	500/1000	100/1000
Maximum security policy	3000	15000
Virtual Firewall	-	100
Fixed interface	2*10GE(SFP+) + 10*GE	2*10GE(SFP+) + 8*GE Combo + 16*GE
Product Form	1U(half)	1U
Dimensions (W×D×H) mm	442*220*43.6	442*420*43.6
Storage	64GB Micro-SD card	64G/240G/960G M.2 Hard disk
Power supply	Single power supply	Standard single power supply, optional dual power supplies

1. Performance is tested under ideal conditions based on RFC2544, 3511. The actual result may vary with deployment environments.
2. SA performances are measured using 100 KB HTTP files.
3. NGFW throughput is measured with Firewall, SA, and IPS enabled; the performance is measured using 100 KB HTTP files.
4. NGFW throughput is measured with Firewall, SA, and IPS enabled; the performance is measured using the Enterprise Mix Traffic Model.
5. The threat protection throughput is measured with Firewall, SA, IPS, and AV enabled; the performance is measured using the Enterprise Mix Traffic Model.
6. SSL VPN throughput is measured using TLS v1.2 with AES128-SHA.
7. NGFW throughput is measured with Firewall, SA, IPS, and AV enabled, the performances are measured using 100 KB HTTP files.
8. SSL inspection throughput is measured with IPS-enabled and HTTPS traffic using TLS v1.2 with TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256.

*SA: indicates service awareness.

Ordering Information

Product	Model	Description
USG6000F-S125	USG6000F-S125-AC	Assembling Components, USG6000F-S125-AC, USG6000F-S125-AC, USG6000F-S125-AC Host (10*GE RJ45 + 2*10GE SFP+, 1*Built-in AC Power, Include SSL VPN 100 users)
USG6000F-S200	USG6000F-S200-AC	Assembling Components, USG6000F-S200-AC, USG6000F-S200-AC, USG6000F-S200-AC Host (16*GE RJ45 + 8*GE COMBO + 2*10GE SFP+, 1 AC power, Include SSL VPN 100 Users)
Basic License		
Number of concurrent SSL VPN users	LIC-USG6KF-SSLVPN-20	Software Charge, USG6000F-S, LIC-USG6KE-SSLV PN-20, Quantity of SSL VPN Concurrent Users (20 Users), Electronic
	LIC-USG6KF-SSLVPN-50	Software Charge, USG6000F-S, LIC-USG6KE-SSLV PN-50, Quantity of SSL VPN Concurrent Users (50 Users), Electronic
NGFW License		
Threat protection capabilities Package	LIC-USG6000F-S125-TP-O-1Y	Software Charge, USG6000F-S125, LIC-USG6000F-S125-TP-O-1Y, Threat Protection (Intrusion Prevention and Botnet Detection + Antivirus + Online Behavior Management + Threat Information Services) 1 Year (Applies to USG6000F-S125), Electronic
	LIC-USG6000F-S125-TP-O-3Y	Software Charge, USG6000F-S125, LIC- USG6000F-S125-TP-O-1Y, Threat Protection (Intrusion Prevention and Botnet Detection + Antivirus + Online Behavior Management + Threat Information Services) 3 Year (Applies to USG6000F-S125), Electronic
	LIC-USG6000F-S200-TP-O-1Y	Software Charge, USG6000F-S200, LIC-USG6000F-S200-TP-O-1Y, Threat Protection (Intrusion Prevention and Botnet Detection + Antivirus + Online Behavior Management + Threat Information Services) 1 Year (Applies to USG6000F-S200), Electronic
	LIC-USG6000F-S200-TP-O-3Y	Software Charge, USG6000F-S200, LIC-USG6000F-S200-TP-O-1Y, Threat Protection (Intrusion Prevention and Botnet Detection + Antivirus + Online Behavior Management + Threat Information Services) 3 Year (Applies to USG6000F-S200), Electronic
Advanced Threat Protection Feature Pack (IPS, AV, URL)	LIC-USG6000F-S125-ATP-O-1Y	Software Charge, USG6000F-S125, LIC-USG6000F-S125-ATP-O-1Y, Intrusion Prevention and Botnet Detection + Antivirus + URL + Online Behavior Management + Threat Information Services 1 Year (Applies to USG6000F-S125), Electronic
	LIC-USG6000F-S125-ATP-O-3Y	Software Charge, USG6000F-S125, LIC-USG6000F-S125-ATP-O-1Y, Intrusion Prevention and Botnet Detection + Antivirus + URL + Online Behavior Management + Threat Information Services 3 Year (Applies to USG6000F-S125), Electronic

Product	Model	Description
	LIC-USG6000F-S200-ATP-O-1Y	Software Charge, USG6000F-S200, LIC-USG6000F-S200-ATP-O-1Y, Intrusion Prevention and Botnet Detection + Antivirus + URL + Online Behavior Management + Threat Information Services 1 Year (Applies to USG6000F-S200), Electronic
	LIC-USG6000F-S200-ATP-O-3Y	Software Charge, USG6000F-S200, LIC-USG6000F-S200-ATP-O-1Y, Intrusion Prevention and Botnet Detection + Antivirus + URL + Online Behavior Management + Threat Information Services 3 Year (Applies to USG6000F-S200), Electronic
Enterprise Security Protection	LIC-USG6KF-S200-ESP-1Y	Software Charge, USG6000F-S200-LIC-USG6KF-S200-ESP-1Y-OVS-Enterprise Security Protection Function Package: 1 Year (IPS, Antivirus, URL, Industrial Control Security, Online Behavior Management, and Threat Information Service) (Applicable to USG6000F-S200 Outside China)-Electronic
	LIC-USG6KF-S200-ESP-3Y	Software Charge, USG6000F-S200-LIC-USG6KF-S200-ESP-3Y-OVS-Enterprise Security Protection Function Package: 3 Years (IPS, Antivirus, URL, Industrial Control Security, Online Behavior Management, and Threat Information Service) (Applicable to USG6000F-S200 Outside China)-Electronic

Note: Some parts of this table list the sales strategies in different regions. For more information, please contact your Huawei representative.