HUAWEI eKitEngine USG6000F-S Series AI Firewalls

HUAWEI eKitEngine USG6000F-S Series AI Firewalls

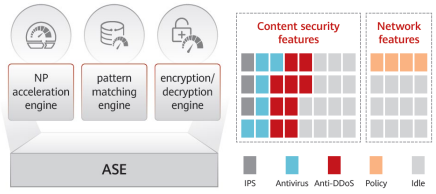
As digitalization is sweeping the world, extensive connections, explosive growth of data, and booming intelligent applications are profoundly changing the way we live and work. Enterprise services are going digital and moving to the cloud, which promotes the transformation of enterprise networks while 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 are next-generation AI firewalls that feature intelligent defense, outstanding performance, and simplified O&M, effectively addressing the preceding challenges. The eKitEngine USG6000F-S Series AI firewalls use intelligence technologies to enable border defense to accurately block known and unknown threats. Equipped with multiple built-in security-dedicated acceleration engines, the eKitEngine USG6000F-S Series AI 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.

HUAWEI

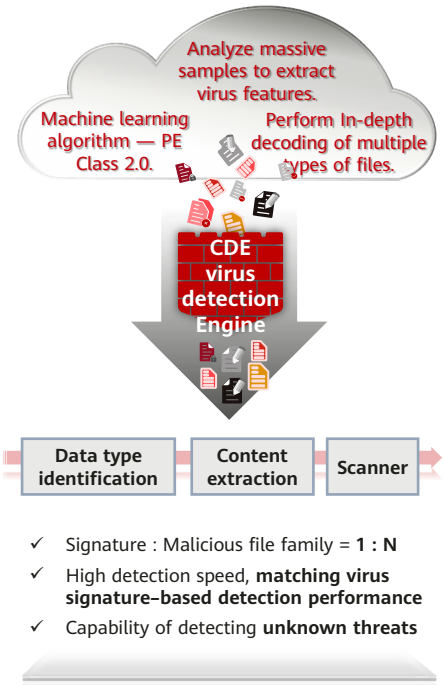
01 Product Highlights

Excellent performance



By leveraging fresh-new hardware and software architectures of forwarding and control separation, the 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 eKitEngine 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



- ✓ Signature : Malicious file family = **1 : N**
- ✓ High detection speed, **matching virus signature–based detection performance**
- ✓ Capability of detecting **unknown threats**

The 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. eKitEngine USG6000F-S Series also support to detect unknown threats by interworking with sandbox.

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.

eKitEngine USG6000F-S Series supports to detect and defend malware spreading and network attacks, like Worm, Virus, Trojan-horse, Spyware, etc. malware spreading and botnet, DoS/DDoS, SQL injection, cross site attack,ransomware,etc.

Simplified O&M

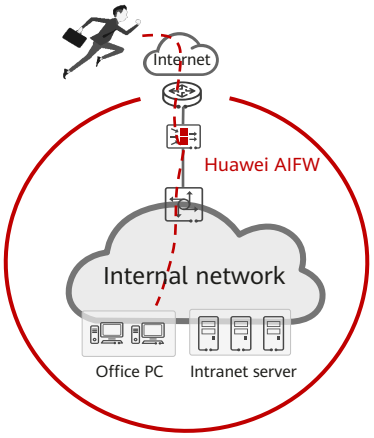
The eKitEngine USG6000F-S Series AI firewalls provides a brand-new web UI, which intuitively visualizes threats as well as displays key information such as device status, alarms, traffic, and threat events. With multi-dimensional data drilling, the web UI offers optimal user experience, enhanced usability,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

The eKitEngine USG6000F-S Series 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.

The eKitEngine USG6000F-S Series can also be managed by NCE-Campus, and NCE-Campus can also support to manage switch, AR, POL device at the same time, even third party devices.

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.

02 Deployment

Small data center border protection

- Firewalls are deployed at egresses of data centers, and functions and system resources can be virtualized. The firewall has multiple types of interfaces, such as 10GE, and GE interfaces. Services can be flexibly expanded without extra interface cards.
- The intrusion prevention capability effectively blocks a variety of malicious attacks and delivers differentiated defense based on virtual environment requirements to guarantee data security.
- VPN tunnels can be set up between firewalls and mobile workers and between firewalls and branch offices for secure and low-cost remote access and mobile working.

Enterprise border protection

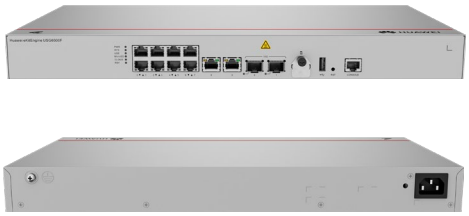
- Firewalls are deployed at the network border. The built-in traffic probe can extract packets of encrypted traffic to monitor threats in encrypted traffic in real time.
- The policy control and data filtering functions of the firewalls are used to monitor social network applications to prevent data breach and protect enterprise networks.

03 Product Appearance

- **Rich access capability** : Ethernet, 5G RU

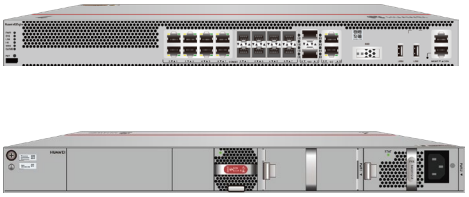
- **Figure 3-1**

eKitEngine USG6000F-S125



- **Figure 3-2**

eKitEngine USG6000F-S150



- **Figure 3-3**

eKitEngine USG6000F-S200

04 Software Features

Feature	Description
Integrated protection	Integrates firewall, VPN, intrusion prevention, antivirus, bandwidth management, Anti-DDoS, and URL filtering functions, and provides a global configuration view and integrated policy management.
Application identification and control	Application identification based on signatures, correlation, and behaviors instead of ports; 6000+ preset applications, which can be further classified; support for user-defined applications; 50+ categories and 20+ risk labels for access control based on categories and labels; automatic update of the application identification signature database
Security policy management	Supports traffic management and control based on the VLAN ID, 5-tuple, security zone, region, application, and time range, and implements integrated content security inspection. Provides predefined templates for common attack defense scenarios to facilitate security policy deployment. Supports interworking with third-party policy management software (FireMon and Algosec) to facilitate security O&M.
Bandwidth management	Manages per-IP bandwidth based on service application identification to guarantee 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.
Intrusion prevention	Obtains the latest threat information in a timely manner and accurately detects and prevents vulnerability exploits; covers tens of thousands of CVE vulnerabilities; prevents the exploit of vulnerabilities (such as those in Windows and Unix/Linux operating systems, databases, Apache, IIS, and Tomcat as well as middleware), web attacks (such as SQL injection, XSS, and RCE), botnets, remote control, and Trojan horses; supports brute force cracking detection based on user behavior; provides 25,000+ predefined signatures and supports user-defined signatures and automatic signature database update; supports attack forensics collection, full-flow packet obtaining (including three-way handshake information), and attack fragment display to facilitate O&M; supports X-Forwarded-For (XFF) field extraction.
Antivirus	Detects malware in files transmitted through protocols like HTTP, FTP, SMTP, POP3, IMAP4, NFS, and SMB; detects Trojan horses, worms, spyware, vulnerability exploits, adware, hacker tools, Rootkit, backdoors, grayware, botnet programs, ransomware, phishing software, cryptojacking software, and web shell programs; supports virus detection for Office files, executable files (Windows/Linux/MacOS), script files, flash files, PDF files, RTF files, web pages, and images; supports attack forensics collection; supports the inspection of archive files of up to 100 nested compression levels in multiple compression formats, such as tar, gzip, zip, rar, and 7z, and supports multiple actions, such as alert, block, add declaration, and attachment deletion.
Advanced malware prevention	The heuristic antivirus engine uses detection technologies such as AI, semantic analysis, and Emulator, coupled with threat and reputation information, to detect packed malware, script morphing, and malware embedded in compound documents. It can detect billions of malware variants and supports automatic update of the signature database. In addition, it can send suspicious files to the local or cloud sandbox for further inspection to detect zero-day malware.
Web security	The URL category database on the cloud contains 560 million URLs in over 130 categories, such as news, games, gambling, drugs, and malicious web pages. URLs cover over 100 languages, and key categories of URLs cover over 20 languages. The URL category query servers are deployed in multiple countries/regions to provide high-speed and low-latency category query services. User-defined URL/host whitelist and blacklist are supported. HTTPS traffic can be filtered without decryption.

Feature	Description
Web security	TLS/SSL traffic can be decrypted before filtering. HTTP/2 and QUIC traffic can be filtered, and URL categories can be imported in batches. Supports Safe Search enforcement across five major search engines: YouTube, Bing, Google, Yahoo, and Yandex, with mandatory filtering of illegal or inappropriate content in search results. URL access can be controlled based on users/user groups, time ranges, and security zones to precisely manage users' online behaviors.
DNS security	Based on massive threat information, technologies such as AI and knowledge graph are used to detect malicious DNS requests, including C&C domain names, DGA-generated domain names, compromised sites, and malicious domain names such as cryptojacking, ransomware, and phishing domain names. The local malicious domain name database supports a maximum of 2 million malicious domain names. DNS category-based filtering, DNS safe search, and DNS redirection (sinkholing) are also supported.
Anti-botnet/spyware	Supports the detection and prevention of viruses and advanced malware, such as botnets, Trojan horses, worms, remote control tools, and spyware, and prevents the download of malware; quickly detects malicious traffic like C&C based on signatures, IP addresses, and domain reputation information; displays the roles of communication parties in botnet attack logs.
Threat information	Huawei Intelligent Security Center leverages multiple AI algorithms and expert analysis to generate massive threat information about IP addresses, domain names, URLs, and files on a daily basis. The threat information is automatically synchronized to devices for threat detection to quickly block emerging attacks. In addition, it can interconnect with third-party threat information sources to enrich inspection rules.
Anti-DDoS	Uses technologies such as source IP address detection, fingerprint detection, and dynamic traffic limiting to defend against over 10 common DDoS attacks and over 20 single-packet attacks, such as SYN flood, UDP flood, ICMP flood, HTTP flood, HTTPS flood, DNS flood, and SIP flood attacks, and supports traffic baseline learning and IP reputation-based filtering.(USG6000F-S125 not support)
Mail filtering	Supports mail address filtering (covering the sender and recipient addresses) and SMTP mail sending rate limiting.
DLP	Supports identification of 100+ real file types, user-defined file name extensions, and file type-based upload/download control; supports keyword filtering for Office documents, web pages, code, and TXT files; supports user-defined keywords, regular expressions, and weight configuration.
O&M capability	Supports telemetry to automatically read information from hardware, such as fans, power modules, optical modules, Ethernet ports, temperature sensors, and drivers, and sends interface traffic statistics, CPU usage, and memory usage to the collector.
PPPoE	Functions as a PPPoE client to provide Internet access services, including user authentication and authorization and dynamic IP address allocation.
Posture compliance check	Supports Operating System Version Check, Operating System Patch Check, Antivirus Software Check, Firewall Check, Running Process Check, File Security Check, Registry Check, Port Check, Anti-Screenshot, Anti Double Redirect, and Prevents Nested Remote Desktop Connections.

Feature	Description
Behavior audit	Audits and regulates common user online behaviors, including FTP operations (upload, download, and command), HTTP operations (posting, search, and browsing), DNS, Telnet, SNMP, and email sending and receiving operations.
Intelligent uplink selection	Supports service-specific PBR and intelligently selects the optimal link based on multiple types of load balancing criteria (such as the bandwidth ratio and link health status) in multi-ISP scenarios.
VPN encryption	Supports various highly reliable VPN features, such as IPsec VPN, SSL VPN, and GRE, and multiple encryption algorithms, such as DES, 3DES, AES, SHA, SM2, SM3, and SM4.
SSL-encrypted traffic inspection	Detects and defends against threats hidden in TLS/SSL-encrypted traffic, performs application-layer protection, such as intrusion prevention, antivirus, data filtering, and URL filtering, on decrypted TLS/SSL traffic, and supports URL category whitelist.
SSL offloading	Replaces the server to implement SSL encryption and decryption, reducing the server load and implementing load balancing of HTTP traffic.
Diversified reports	Provides visualized and multi-dimensional reports by IP address, application, time, traffic, or threat.
Security virtualization	Supports virtualization of multiple types of security services, including firewall, intrusion prevention, antivirus, and VPN services; allows users to separately conduct personalized management on the same physical device.
Routing	Supports multiple types of IPv4/IPv6 routing protocols, such as RIP, OSPF, BGP, IS-IS, RIPng, OSPFv3, BGP4+, and IPv6 IS-IS.
IP multicast	Supports IPv4 Layer 3 multicast protocols, such as IGMP, MSDP, and PIM, and provides point-to-multipoint services to reduce bandwidth consumption.
Server load balancing	Supports IPv6, Layer 4/Layer 7 server load balancing, and multiple session persistence methods such as source IP address-based and HTTP cookie-based session persistence; supports SSL offloading and encryption; combines services and security policies to improve service security; supports health check based on multiple protocols such as TCP, RADIUS, DNS, and HTTP to detect server status changes promptly.
Deployment and reliability	Supports transparent (Layer 2), routing (Layer 3), tap, and hybrid working modes and high availability (HA), including the Active/Active and Active/Standby modes.
Security center	The built-in asset identification module can identify assets such as Windows, Linux, Android, and iOS assets and cameras, perform correlation analysis on threat logs and assets, and display asset risk assessment results and the entire kill chain.
SRv6	Supports IS-IS for SRv6, BGP for SRv6, SRv6 BE, SRv6 TE policy, SRv6 midpoint protection, SRv6 microloop avoidance, SRv6 OAM, SRv6 SRH compression, SRv6 TI-LFA FRR, and EVPN L3VPN.
Secure SD-WAN	Provides a built-in secure SD-WAN solution for low-cost and business-level Internet links. Supports zero-touch provisioning (ZTP) through email to complete device provisioning in minutes without requiring technical skills. Supports forward error correction (FEC) to prevent pixelated display and video freezing at a 30% packet loss rate; supports real-time link switching based on link quality ensure key application experience. Supports multi-link routing and dual-CPE flexible networking to ensure uninterrupted connections for site services; supports E2E IPsec encryption to ensure secure service transmission.
User authentication	Supports multiple authentication modes for Internet access users, including local Portal authentication and single sign-on (SSO). In local Portal authentication, the built-in Portal page of the device can be pushed to users, and the account and password entered on the Portal page by a user can be sent to the local database or RADIUS, HWTACACS, AD, or LDAP authentication server for authentication. SSO includes RADIUS SSO and Agile Controller (NCE-Campus) SSO.

05 Specifications

• System Performance and Capacity

Model	USG6000F-S125	USG6000F-S150	USG6000F-S200
Recommend Number of Users	600	1000	2500
IPv4Firewall Throughput[1] (1518/512/64-byte, UDP)	8/8/3.6 Gbps	12/12/4 Gbps	16/16/5 Gbps
IPv6 Firewall Throughput[1] (1518/512/84-byte, UDP)	8/8/3.6 Gbps	12/12/4 Gbps	16/16/5 Gbps
Secure SD-WAN EVPN Throughput(1400/512 byte,UDP) [9]	5/5 Gbps	9/6.6 Gbps	10/6.8 Gbps
Secure SD-WAN EVPN tunnels	200	200	200
Firewall Latency (64-byte, UDP)	18 μs	18 μs	18 μs
Firewall Latency (64-byte, UDP) [8]	7 μs	7 μs	7 μs
Concurrent Sessions (HTTP1.1)[1]	1,000,000	4,000,000	4,000,000
New Sessions/Second (HTTP1.1)[1]	50,000	80,000	120,000
FW + SA* Throughput[2]	2 Gbps	2.8 Gbps	4.5 Gbps
NGFW Throughput (HTTP 100K) [3]	1.7 Gbps	2.1 Gbps	3 Gbps
NGFW Throughput(Enterprise Mix)[4]	1.2 Gbps	1.3 Gbps	2 Gbps
Threat Protection Throughput (FW + SA + IPS + AV, HTTP 100K)[10]	1.4 Gbps	1.8 Gbps	2.5 Gbps
Threat Protection Throughput (Enterprise Mix)[5]	1 Gbps	1.2 Gbps	1.8 Gbps
IPsec VPN Throughput (AES-256 + SHA256, 1420-byte) [1]	3.7 Gbps	3.5 Gbps	5.6 Gbps
Maximum IPsec VPN Tunnels	2,000	4,000	4,000
SSL VPN Throughput [6]	300Mbps	500Mbps	750Mbps
Concurrent SSL VPN Users *(Default/Maximum)	100/1,000	100/1,600	100/2,000
Security Policies (Maximum)	3,000	15,000	15,000
Virtual Firewalls	20	100	100
URL Filtering: Categories	More than 130		
URL Filtering: URLs	A database of over 560 million URLs in the cloud		
Automated IPS Signature Updates	Yes, an industry-leading security center from Huawei(https://isecurity.huawei.com/security/service/ips)		
Third-Party and Open-Source Ecosystem	Open API for integration with third-party products, providing NETCONF interfaces. Other third-party management software based on SNMP, SSH, and Syslog		
VLANs (Maximum)	4094		
VLANIF Interfaces (Maximum)	4094		

- Performance is tested under ideal conditions based on RFC2544, 3511. The actual result may vary with deployment environments.
- SA performances are measured using 100 KB HTTP files.
- NGFW throughput is measured with Firewall, SA, and IPS enabled; the performance is measured using 100 KB HTTP files.
- NGFW throughput is measured with Firewall, SA, and IPS enabled; the performance is measured using the Enterprise Mix Traffic Model.
- The threat protection throughput is measured with Firewall, SA, IPS, and AV enabled; the performance is measured using the Enterprise Mix Traffic Model.
- SSL VPN throughput is measured using TLS v1.2 with AES128-SHA.
- SSL inspection throughput is measured with IPS-enabled and HTTPS traffic using TLS v1.2 with TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256.
- The data test condition is the interface pair mode .
- The SD-WAN tunnel is packed with GRE over IPSec.
- The threat protection throughput is measured with Firewall, SA, IPS, and AV enabled, the performances are measured using 100 KB HTTP files.

*SA: indicates service awareness.

06 Hardware Specifications

Model	USG6000F-S125	USG6000F-S150	USG6000F-S200
Chassis Height	1 U(half)	1 U	
Dimensions (H x W x D) mm	43.6 x 442 x 220	43.6 x 442 x 420	
Fixed Interface	2*10GE (SFP+) + 10*GE	2*10GE(SFP+) +8*GE Combo+2*GE	2*10GE(SFP+) +8*GE Combo+16*GE
USB Port	1 x USB 3.0	2 x USG3.0	1 x USB 3.0
Weight	2.32 kg	5.46 kg	5.816 kg
External Storage	Optional, 64 GB microSD card available for purchase	Optional, SSD M.2 supported, 64GB/240GB/960GB	
Power Supply (AC)	100V～240V，50Hz/60Hz		
Maximum power consumption of the machine	27.4 W	49.5 W	53.2 W
Power Supplies	Single AC power supply	Dual AC power supplies	
Operating Environment (Temperature/Humidity)	Temperature: 0° C to 45° C Humidity: 5% to 95%, non-condensing		
Non-operating Environment	Temperature: –40° C to +70° C Humidity: 5% to 95%, non-condensing		
Installation Type	Rack		

07 Ordering Information

- **Note:**

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

Product	Model	Description
USG6000F-S125	USG6000F-S125-AC	USG6000F-S125 AC Host (2*10GE (SFP+) + 10*GE, 1 AC power supply)
USG6000F-S150	USG6000F-S150-AC	USG6000F-S150 AC Host (2*10GE(SFP+) +8*GE Combo+2*GE, 1 AC power supply)
USG6000F-S200	USG6000F-S200-AC	USG6000F-S150 AC Host (2*10GE(SFP+) +8*GE Combo+16*GE, 1 AC power supply)
Function License		
SSL VPN	LIC-USG6KF-SSLVPN-20	Quantity of SSL VPN Concurrent Users (20 Users)
	LIC-USG6KF-SSLVPN-50	Quantity of SSL VPN Concurrent Users (50 Users)
NGFW License		
Year of Threat Protection Service (include IPS + AV + Online Behavior Management + Threat Information Services) (1Y/3Y)	LIC-USG6000F-S125-TP -OVS	Threat Protection Subscription Per Year (Applies to USG6000F-S125 Overseas)
	LIC-USG6000F-S150-TP -OVS	Threat Protection Subscription Per Year (Applies to USG6000F-S150 Overseas)
	LIC-USG6000F-S200-TP -OVS	Threat Protection Subscription Per Year (Applies to USG6000F-S200 Overseas)
Year of Advanced Threat Protection Service (include IPS + AV + URL + Online Behavior Management + Threat Information Services) (1Y/3Y)	LIC-USG6000F-S125-ATP -OVS	Advanced Threat Protection Subscription Per Year (Applies to USG6000F-S125 Overseas)
	LIC-USG6000F-S150-ATP -OVS	Advanced Threat Protection Subscription Per Year (Applies to USG6000F-S150 Overseas)
	LIC-USG6000F-S200-ATP -OVS	Advanced Threat Protection Subscription Per Year (Applies to USG6000F-S200 Overseas)
Year of Enterprise Threat Protection Service (include IPS + AV + URL +Industrial Control Security + Online Behavior Management + Threat Information Services) (1Y/3Y)	LIC-USG6000F-S150-ESP -OVS	Enterprise Threat Protection Subscription Per Year (Applies to USG6000F-S150 Overseas)
	LIC-USG6000F-S200-ESP -OVS	Enterprise Threat Protection Subscription Per Year (Applies to USG6000F-S200 Overseas)