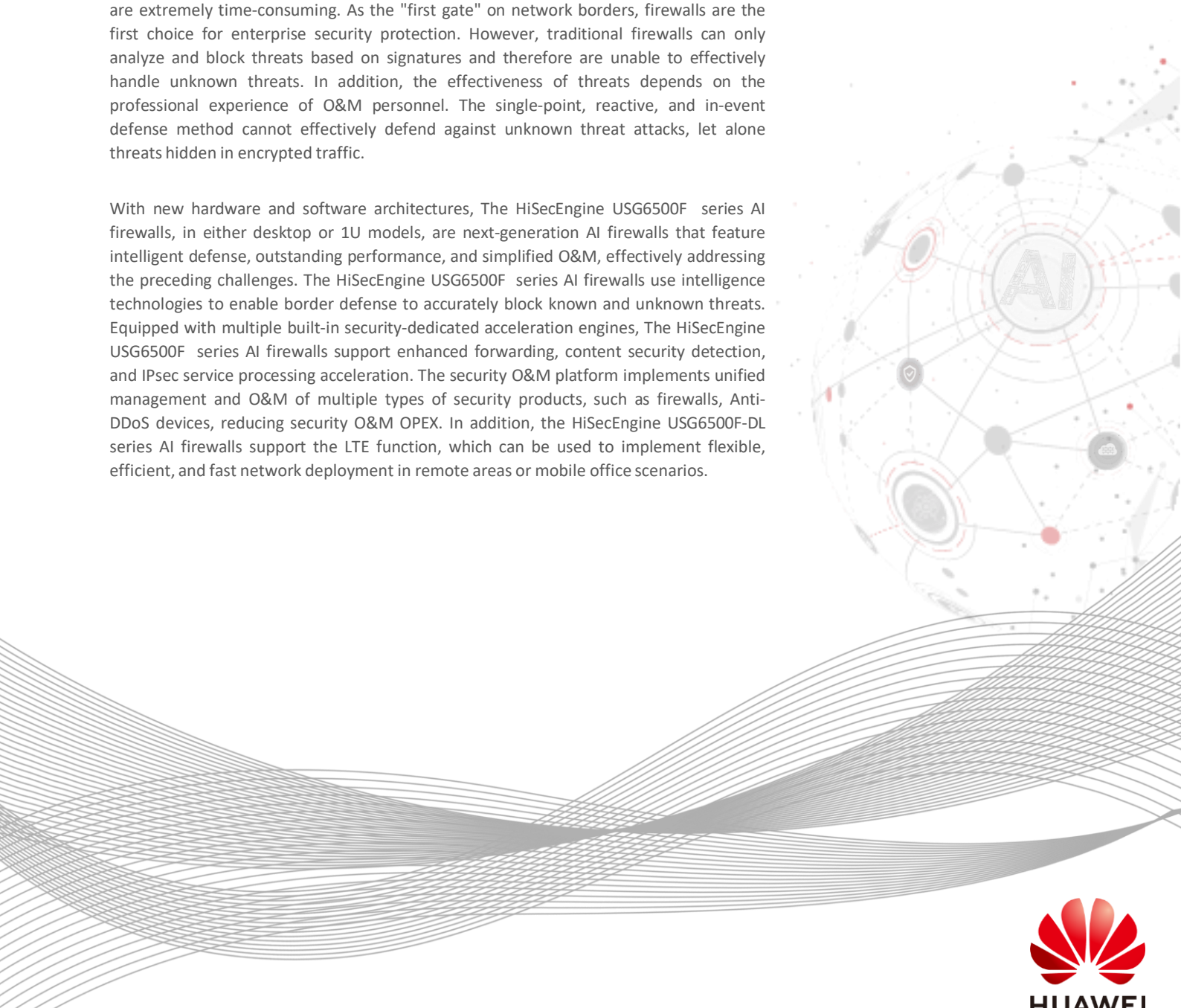
HUAWEI HiSecEngine USG6500F Series AI Firewalls

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.

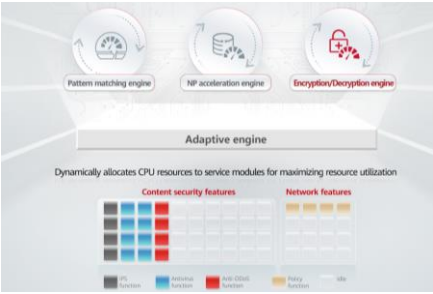
With new hardware and software architectures, The HiSecEngine USG6500F series AI firewalls, in either desktop or 1U models, are next-generation AI firewalls that feature intelligent defense, outstanding performance, and simplified O&M, effectively addressing the preceding challenges. The HiSecEngine USG6500F 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 HiSecEngine USG6500F 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. In addition, the HiSecEngine USG6500F-DL series AI firewalls support the LTE function, which can be used to implement flexible, efficient, and fast network deployment in remote areas or mobile office scenarios.



HUAWEI

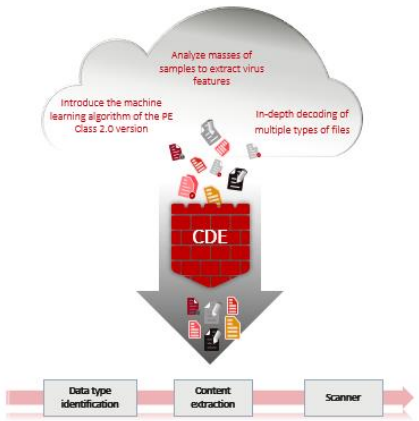
01 Product Highlights

Excellent performance



By leveraging fresh-new hardware and software architectures of forwarding and control separation, the HiSecEngine USG6500F 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 USG6500F series AI firewalls also support 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**
- ✓ Detection speeds are **equivalent to the signature detection performance**
- ✓ Industry-leading **unknown threat** detection capabilities

The HiSecEngine USG6500F series AI firewalls provide content security functions, such as application identification, IPS, antivirus, and URL filtering to protect intranet servers and users against threats. The HiSecEngine USG6000F series AI firewalls 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 content-based detection engine (CDE) powered by intelligent technologies can detect over 100 million malware samples. Coupled with the AI security detection model, the engine performs in-depth malware analysis to quickly detect malicious files and ransomware, improving the threat detection rate.

Simplified O&M

The HiSecEngine USG6500F 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.

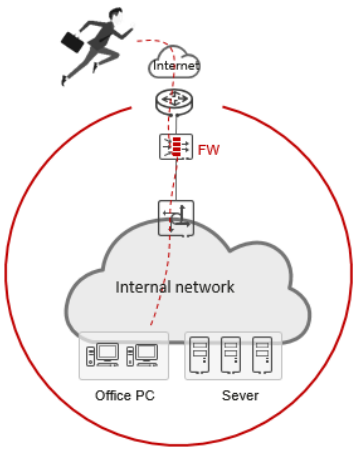
The HiSecEngine USG6500F series AI firewalls can be centrally managed by the security management platform SecoManager, implementing a shift from single-point defense to collaborative network protection. The SecoManager provides policy tuning and intelligent O&M capabilities. It can also manage security

products, such as anti-DDoS devices to quickly eliminate network threats and improve security handling effectiveness.

The HiSecEngine USG6500F series AI firewalls 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.

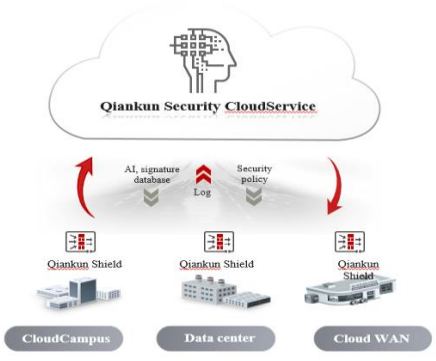
A wide range of network features

Huawei HiSecEngine USG6500F series AI firewalls provide 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.
- Most threats and attacks come from network traffic. Firewalls are deployed at the egress of the local network to interwork with Huawei Qiankun security cloud service to implement automatic threat analysis and handling. This ensures the interconnection between the intranet and extranet, effectively intercepts traffic attacks, and automatically handles external attack sources. Protects enterprise network resources.

Collaboration with Huawei Qiankun Security Cloud Service



- Most threats and attacks come from network traffic. Firewalls are deployed at the egress of the local network to interwork with Huawei Qiankun security cloud service (Qiankun security Cloud availability is subject to regional differences) to implement automatic threat analysis and handling. This ensures the interconnection between the intranet and extranet, effectively intercepts traffic attacks, and automatically handles external attack sources. Protects enterprise network resources.
- By associating with Huawei Qiankun security cloud service, the firewall can obtain security services such as border protection and response on demand. Lightweight deployment and unified cloud O&M effectively reduce hardware stacking and greatly reduce enterprise security investment and O&M difficulties.

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 10G (SFP+), GE (RJ45) and GE(SFP) 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.

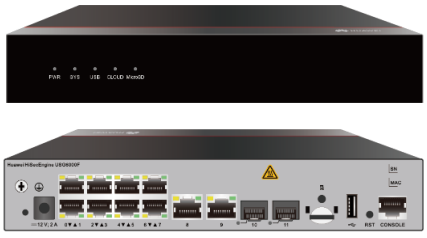
Enterprise border protection

- 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.

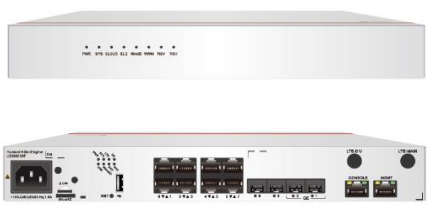
03 Product Appearance

- **Rich access capability :** Ethernet, LTE/5G RU and GPON.
- **Figure**

HiSecEngine USG6510F-D/USG6530F-D



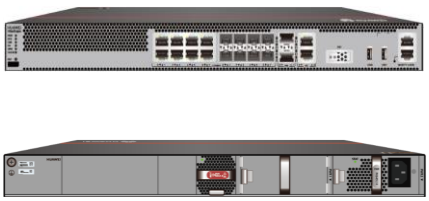
HiSecEngine USG6510F-DL/USG6530F-DL



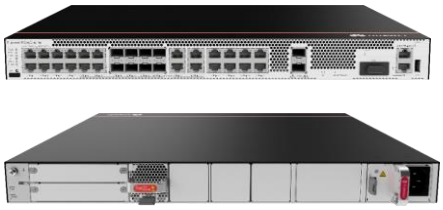
HiSecEngine USG6510F-DPL/ USG6530F-DPL

HiSecEngine USG6560F-D

HiSecEngine USG6525F/USG6555F/USG6565F/USG6585F



HiSecEngine USG6585F-B



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; supports policy self-learning, aggregates traffic matching a security policy, and generates more refined sub-security policies to achieve precise security management.
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 13,000+ 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. The USG6500F-D series supports a maximum of 10000 IPS signatures.
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. 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 and malicious domain name information on the cloud, 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 500,000 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.

OT/IoT security	Supports common industrial control protocols such as Modbus, S7, Profinet, and OPC, identification and control of IoT devices such as cameras, and IoT asset risk assessment. Supports vulnerability detection for IoT devices like cameras and industrial control software and protocols like ICS/SCADA. The traffic probe function, coupled with HiSec Insight situational awareness system, can learn the traffic behavior baseline of IoT assets and detect and evaluate IoT asset risks. 1.For details about the list of supported OT protocols, see https://isecurity.huawei.com/security/wiki/application (Business Systems > Industrial). 2. The USG6500F-D series does not support industrial control protocols. 3. Firewalls are deployed at Level 3.5 or above of the Purdue model.
Flow probe	Collects and parses metadata and attack forensics information, including network-layer metadata (such as IP addresses, ports, and packet characteristics) and application-layer metadata (such as field information obtained after in-depth parsing of protocols like HTTP, DNS, TLS, and SSH), and sends the data to the HiSec Insight security situational awareness platform for further analysis by using algorithms, such as deep learning and machine learning algorithms, to detect potential, unknown, and advanced threats in network traffic. The USG6500F-D series does not support Flow probe.
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. The USG6500F-D series supports only single-packet attack defense.
Mail filtering	Supports email address filtering, real-time blacklist, and filtering by Multipurpose Internet Mail Extensions (MIME) header fields (such as sender, recipient, and subject), and restriction of the number of SMTP mails sent during a period of time.
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.
SaaS access control	Supports SaaS application identification and access control based on signatures, DNS, IP addresses (IP address database of the top 50 SaaS applications), and first packets, and supports traffic steering based on SaaS applications, ensuring good SaaS application experience.
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, link health status, geographic location) 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 (IPv4, IPv6)-encrypted traffic, performs application-layer protection, such as intrusion prevention, antivirus, data filtering, and URL filtering, on decrypted TLS/SSL (IPv4, IPv6) 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.Provides reports, including traffic, threat, mail filtering, bandwidth management, system, policy matching, file blocking, data filtering, and URL filtering reports, and supports report customization and subscription.
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.

Model poisoning detection	Provides ultra-fast scanning of model files in mainstream formats such as ONNX, Pickle, Safetensors, PTH, and Checkpoint to prevent loading of malicious models that could lead to asset theft or damage.
Prompt injection protection	Filters model input content using static rules or user-defined regular expressions, and identifies prompt injection patterns using semantic analysis and AI techniques, preventing attacks such as SQL injection, XSS, and RCE.
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.
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.
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.
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.
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.
Forward proxy	Serves as a proxy server for intranet terminals that have passed user authentication and security policy check so that they can access the Internet. It can also manage the online behaviors of users and send logs to the log server. It supports HTTP and HTTPS.
WebMaster	An embedded network management system that offers a visualized and easy-to-use human-machine interface for network-wide visualization, one-click network-level service provisioning, and NE management. It also provides automatic network management capabilities, such as automatic deployment, diagnosis, and troubleshooting.

Firewall Interworking with Huawei Qiankun Security CloudService

Service	Description
Border protection and response service	Intrusion detection and prevention: Leverages signatures to block application-layer attacks, terminates the transfer of phishing emails and malware (such as viruses and Trojan horses), detects compromised hosts on the internal network, and disconnects these hosts from the Internet to protect the security and stability of customer services.
	Automatic event analysis: Combines intelligent analysis and manual analysis by experts to analyze security events to ensure the accuracy of attack blocking and security alarms and optimize attack identification rules.
	Whitelist and blacklist: Supports whitelist and blacklist configuration on the Portal or app to protect services from threats.
	Periodic security reports: Generates weekly and monthly reports on security protection events and sends the reports to users by email.
	Emergency notification: Identifies emergencies from security events and sends notifications to users via SMS and email.

05 Specifications

- **System Performance and Capacity**

Model	USG6510F-D	USG6530F-D	USG6560F-D	USG6510F-DL USG6510F-DPL	USG6530F-DL USG6530F-DPL
IPv4 Firewall Throughput[1] (1518/512/64-byte, UDP)	6/6/3.6 Gbps	12/12/3.6 Gbps	12/12/3.6 Gbps	6/6/3.6 Gbps	12/12/3.6 Gbps
IPv6 Firewall Throughput[1] (1518/512/84-byte, UDP)	6/6/3.6 Gbps	12/12/3.6 Gbps	12/12/3.6 Gbps	6/6/3.6 Gbps	12/12/3.6 Gbps
Secure SD-WAN Throughput[9] (1400/512 byte,UDP)	5/5 Gbps	6/6 Gbps	6/6.6 Gbps	5/5 Gbps	6/6 Gbps
SD-WAN EVPN max tunnels	200	200	200	200	200
Firewall Throughput (Packets Per Second)	5.4 Mpps	5.4 Mpps	5.4 Mpps	5.4 Mpps	5.4 Mpps
FW + SA* Throughput[2]	1.8 Gbps	2.2 Gbps	3 Gbps	1.8 Gbps	2.2 Gbps
NGFW Throughput (HTTP 100K)[3]	1.6 Gbps	1.8 Gbps	2.2Gbps	1.6 Gbps	1.8 Gbps
NGFW Throughput (Enterprise Mix)[4]	1 Gbps	1.2 Gbps	1.3 Gbps	1 Gbps	1.2 Gbps
Threat Protection Throughput (HTTP 100K)[7]	1.3 Gbps	1.5 Gbps	2 Gbps	1.3 Gbps	1.5 Gbps
Threat Protection Throughput (Enterprise Mix)[5]	800 Mbps	1 Gbps	1.2 Gbps	800 Mbps	1 Gbps
Concurrent Sessions	800,000	1,000,000	1,000,000	800,000	1,000,000
IPv6 Concurrent Sessions[1]	200,000	500,000	500,000	200,000	500,000

Model	USG6510F-D	USG6530F-D	USG6560F-D	USG6510F-DL USG6510F-DPL	USG6530F-DL USG6530F-DPL
New Sessions/Second (HTTP1.1)[1]	40,000/s	50,000/s	50,000/s	40,000/s	50,000/s
IPv6 New Sessions/Second (HTTP1.1)[1]	8,000/s	30,000/s	30,000/s	8,000/s	30,000/s
IPsec VPN Throughput[1] (AES-256 + SHA256, 1420-byte)	2 Gbps	3.7 Gbps	3.7 Gbps	2 Gbps	3.7 Gbps
Maximum IPSec VPN Tunnels (GW/Client to GW)	1,000	2,000	2,000	1,000	2,000
SSL Inspection Throughput[8]	0.8 Gbps	1.3 Gbps	1.5 Gbps	0.8 Gbps	1.3 Gbps
SSL VPN Throughput[6]	200 Mbps	300 Mbps	300 Mbps	200 Mbps	300 Mbps
Concurrent SSL VPN Users (Default/Maximum)	100/300	100/1,000	100/1,000	100/300	100/1,000
Firewall Policies (Maximum)	3,000	3,000	3,000	3,000	3,000
Virtual Firewalls	10	20	20	10	20
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				

Model	USG6525F	USG6555F	USG6565F	USG6585F	USG6585F-B
IPv4 Firewall Throughput[1] (1518/512/64-byte, UDP)	2.5/2.5/2.5 Gbps	5/5/3.6 Gbps	7/7/3.6 Gbps	9/9/4 Gbps	20/18/5 Gbps
IPv6 Firewall Throughput[1] (1518/512/84-byte, UDP)	2.5/2.5/2.5 Gbps	5/5/3.6 Gbps	7/7/3.6 Gbps	9/9/4 Gbps	20/18/5 Gbps
Secure SD-WAN Throughput[9] (1400/512 byte,UDP)	2.5/2.5 Gbps	5/5 Gbps	6/6 Gbps	9/6.6 Gbps	10/6.8 Gbps
SD-WAN EVPN max tunnels	200	200	200	200	200
Firewall Throughput (Packets Per Second)	3.75 Mpps	5.4 Mpps	5.4 Mpps	6 Mpps	7.5 Mpps
FW + SA* Throughput[2]	2.2 Gbps	3 Gbps	3 Gbps	3 Gbps	4.5 Gbps
NGFW Throughput (HTTP 100K)[3]	1.8 Gbps	2.1 Gbps	2.2 Gbps	2.2 Gbps	3.3 Gbps
NGFW Throughput (Enterprise Mix) [4]	1.2 Gbps	1.2 Gbps	1.2 Gbps	1.3 Gbps	2 Gbps
Threat Protection Throughput (HTTP 100K)[7]	1.5 Gbps	1.8 Gbps	2 Gbps	2 Gbps	3 Gbps
Threat Protection Throughput (Enterprise Mix)[5]	1 Gbps	1 Gbps	1.1 Gbps	1.2 Gbps	1.8 Gbps
Concurrent Sessions	3,000,000	4,000,000	4,000,000	4,000,000	4,000,000
IPv6 Concurrent Sessions[1]	3,000,000	3,000,000	3,000,000	3,000,000	3,000,000
New Sessions/Second (HTTP1.1)[1]	80,000	80,000	80,000	80,000	120,000
IPv6 New Sessions/Second (HTTP1.1)[1]	80,000	80,000	80,000	80,000	120,000
IPsec VPN Throughput[1] (AES-256 + SHA256, 1420-byte)	2.5 Gbps	3.7 Gbps	3.7 Gbps	3.7 Gbps	5.6 Gbps
Maximum IPSec VPN Tunnels (GW/Client to GW)	4,000	4,000	4,000	4,000	4,000
SSL Inspection Throughput[8]	1.5 Gbps	1.5 Gbps	1.5 Gbps	1.5 Gbps	1.9 Gbps

Model	USG6525F	USG6555F	USG6565F	USG6585F	USG6585F-B
SSL VPN Throughput[6]	300 Mbps	500 Mbps	500 Mbps	500 Mbps	750 Mbps
Concurrent SSL VPN Users (Default/Maximum)	100/1,000	100/2,000	100/2,000	100/2,000	100/2,000
Firewall Policies (Maximum)	15,000				
Virtual Firewalls	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				

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. The threat protection 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 with 50% TLS traffic using an average of HTTPS sessions of different cipher suites.
9. The SD-WAN tunnel is packed with GRE over IPSec.

*SA: indicates service awareness.

06 Hardware Specifications

Model	USG6510F-D	USG6530F-D	USG6510F-DL
Chassis Height	Desktop		
Dimensions (W x D x H) mm	250 x 210 x 43.6		320 x 220 x 43.6
Fixed Interface	10*GE RJ45 + 2*GE SFP	10*GE RJ45 + 2*10GE SFP+	4*GE SFP + 8*GE RJ45 + LTE
USB Port	1 x USB 2.0		
Weight	1.55 kg		2.34 kg
Hardware	Optional, 64 GB microSD card available for purchase		
Power Supply(AC)	100 V to 240 V, 50 Hz/60 Hz		
Maximum power consumption of the machine	23.67 W	22.5 W	34.1 W
Power Supplies	Single power supply		
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		

Model	USG6510F-DPL	USG6530F-DL	USG6530F-DPL	USG6560F-D
Chassis Height	Desktop			
Dimensions (W x D x H) mm	320 x 220 x 43.6			
Fixed Interface	4*GE SFP + 8*GE RJ45 + LTE（Support 4*PoE）	2*10GE SFP+ + 2*GE SFP + 8*GE RJ45 + LTE	2*10GE SFP+ + 2*GE SFP + 8*GE RJ45 + LTE（Support 4*PoE）	2*10GE SFP+ + 2*GE SFP+8*GE RJ45
USB Port	1 x USB 2.0			
Weight	2.6 kg	2.34 kg	2.6 kg	2.29 kg
Hardware	Optional, 64 GB microSD card available for purchase			
Power Supply(AC)	100 V to 240 V, 50 Hz/60 Hz			
Maximum power consumption of the machine	35.7 W	34.1 W	35.7 W	29.4W
Power Supplies	Single power supply			
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			

Model	USG6525F	USG6555F	USG6565F	USG6585F	USG6585F-B
Chassis Height	1 U				
Dimensions (W x D x H) mm	442 × 420 × 43.6				
Fixed Interface	2*GE RJ45 + 8*GE COMBO + 2*10GE SFP+				16*GE RJ45 + 8*GE COMBO + 2*10GE SFP+
USB Port	2 x USB 2.0				1 × USB 2.0
Weight	5.46 kg				5.816 kg
Hardware	Optional, M.2 SSD (64 GB/240 GB/960GB), hot-swappable				
Power Supply	100 V to 240 V, 50 Hz/60 Hz				
Maximum power consumption of the machine	36.8 W				53.2 W
Power Supplies	Optional dual power modules for 1+1 redundancy				
Operating Environment	Temperature: 0° C to 45° C Humidity: 5% to 95%, non-condensing				
Storage environment	Temperature: –40° C to +70° C Humidity: 5% to 95%, non-condensing				

07 Ordering Information

- **Note：**
  - **The ordering information of USG6510F-DL/USG6530F-D/USG6530F-DL/ USG6560F-D is the same as USG6510F-D; However, the USG6500F-D series does not support the license for Malicious Traffic AI Detection Engine Upgrade.**
  - **The ordering information of USG6530F-DPL is the same as USG6530F-DPL;**
  - **The license information of USG6555F/USG6565F/USG6585F/USG6585F-B is the same as USG6525F;**
  - **The four models USG6510F-D/USG6530F-D/USG6555F/USG6585F support Qiankun Security Cloud Service;**
  - **Some parts of this table list the sales strategies in different regions. For more information, please contact your Huawei representative.**

Product	Model	Description
USG6510F-D	USG6510F-D-AC	USG6510F-D AC host (10*GE RJ45+2*GE SFP,1*Adapter)
USG6510F-DPL	USG6510F-DPL-AC	USG6510F-DPL AC Host(4*GE SFP+8*GE RJ45+ LTE, 1*Adapter, include SSL VPN 100 users); Supports PoE/PoE+/PoE++, Maximum power supply capability:150W.
USG6525F	USG6525F-AC	USG6525F AC host (2*GE RJ45 + 8*GE COMBO + 2*10GE SFP+, 1 AC power)
	USG6525F-DC	USG6525F DC host (2*GE RJ45 + 8*GE COMBO + 2*10GE SFP+)
Function License		
SSL VPN	LIC-USG6KF-SSLVPN-100	Quantity of SSL VPN Concurrent Users (100 Users)
	LIC-USG6KF-SSLVPN-200	Quantity of SSL VPN Concurrent Users (200 Users)
	LIC-USG6KF-SSLVPN-500	Quantity of SSL VPN Concurrent Users (500 Users)
	LIC-USG6KF-SSLVPN-1000	Quantity of SSL VPN Concurrent Users (1000 Users)
	LIC-USG6KF-SSLVPN-2000	Quantity of SSL VPN Concurrent Users (2000 Users)
	LIC-USG6KF-SSLVPN-5000	Quantity of SSL VPN Concurrent Users (5000 Users)
NGFW License		
IPS Update Service	LIC-USG6525F-IPS-1Y	IPS Update Service Subscribe Per Year (Applies to USG6525F)
URL Filtering Update Service	LIC-USG6525F-URL-1Y	URL Update Service Subscribe Per Year (Applies to USG6525F)
Antivirus Update Service	LIC-USG6525F-AV-1Y	AV Update Service Subscribe Per Year (Applies to USG6525F)
Threat Protection Bundle (IPS, AV, URL)	LIC- USG6510F-D -TP-1Y	Threat Protection Subscription Per Year (Applies to USG6510F-D Overseas)
	LIC-USG6510F-DPL-TPU-1Y	Threat Protection Database Upgrade Service (Applies to USG6510F-D), Per Device, Per Year
	LIC-USG6525F-TP-1Y	Threat Protection Subscription Per Year (Applies to USG6525F Overseas)
Malicious Traffic AI Detection Engine Upgrade	LIC-USG6525F-MTAI	Malicious Traffic AI Detection upgrade Per Year(Applies to USG6525F)
IPv6+	LIC-6500F-IPv6+-LIC	IPv6+ Feature (includes SRv6, channel subinterface, iFit) (Applies to USG6500F)
Industrial Protocol	LIC-USG6525F-ICS-1Y	Industrial Control Security Service Subscribe Per Year (Applies to USG6525F)
N1 License		
USG6510F-D	N1- USG6510F-D -F-Lic	N1-USG6510F-D Foundation, Per Device
	N1- USG6510F-D -F-SnS1Y	N1-USG6510F-D Foundation, SnS, Per Device, Per Year
USG6510F-DPL	N1-USG6510F-DPL-F-Lic	N1-USG6510F-DPL Foundation, Per Device
	N1-USG6510F-DPL-A-Lic	N1-USG6510F-DPL Advanced, Per Device
	N1-USG6510F-DPL-F-SnS1AY	N1-USG6510F-DPL Foundation, SnS, Per Device, Per Year
	N1-USG6510F-DPL-A-SnS1AY	N1-USG6510F-DPL Advanced, SnS, Per Device, Per Year
USG6525F	N1-USG6525F-F-Lic	N1-USG6525F Foundation, Per Device
	N1-USG6525F-F-SnS1Y	N1-USG6525F Foundation, SnS, Per Device, Per Year
	N1-USG6525F-A-Lic	N1-USG6525F Advanced, Per Device
	N1-USG6525F-A-SnS1Y	N1-USG6525F Advanced, SnS, Per Device, Per Year
QianKun Cloud Deployment License		
USG6510F-D	N1-C-USG6510F-D-F-Lic	Cloud Deployment Model Foundation, Per Device,1 Year
	LIC-USG6510F-D-BA-1Y	Border Protection and Response - Threat automatic blocking (Applies to USG6510F-D), Per Device, 1 Year
	LIC-USG6510F-D-TPU-1Y	Threat Protection Database Upgrade Service (Applies to USG6510F-D), Per Device, 1 Year
USG6510F-DPL	N1-C-USG6510F-DPL-F-Lic	Cloud Deployment Model Foundation, Per Device,1 Year
	LIC-USG6510F-DPL-BA-1Y	Border Protection and Response - Threat automatic blocking (Applies to USG6525F), Per Device, 1 Year
	LIC-USG6510F-DPL-TPU-1Y	Threat Protection Database Upgrade Service (Applies to USG6525F), Per Device, 1 Year

QianKun Cloud Deployment License		
USG6525F	N1-C-USG6525F-F-Lic	Cloud Deployment Model Foundation, Per Device,1 Year
	LIC-USG6525F-BA-1Y	Border Protection and Response - Threat automatic blocking (Applies to USG6525F), Per Device, 1 Year
	LIC-USG6525F-TPU-1Y	Threat Protection Database Upgrade Service (Applies to USG6525F), Per Device, 1 Year
Qiankun OP mode		
USG6510F-D	LIC-USG6510F-D-TPU-1Y	Border Protection and Response - Threat automatic blocking (Applies to USG6510F-D), Per Device, 1 Year
USG6510F-DPL	LIC-USG6510F-DPL-TPU-1Y	Threat Protection Database Upgrade Service (Applies to USG6510F-DPL), Per Device, 1 Year
USG6525F	LIC-USG6525F-TPU-1Y	Threat Protection Database Upgrade Service (Applies to USG6525F), Per Device, 1 Year
N1 SASE Branch Interconnection license		
USG6510F-D	N1-USG6510F-D-S-S-Lic	N1 SASE Branch Interconnection Standard Package (Package for USG6510F-D)
	N1-USG6510F-D-S-S-S1Y	N1 SASE Branch Interconnection Standard Package (Package for USG6510F-D),Per Device,1 Year
USG6510F-DPL	N1-USG6510F-DPL-S-S-Lic	N1 SASE Branch Interconnection Standard Package(Package for USG6510F-DPL)
	N1-USG6510F-DPL-S-S-S1Y	N1 SASE Branch Interconnection Standard Package(Package for USG6510F-DPL),Per Device,1 Year
USG6525F	N1-USG6525F-S-S-Lic	N1 SASE Branch Interconnection Standard Package(Package for USG6525F)
	N1-USG6525F-S-S-S1Y	N1 SASE Branch Interconnection Standard Package(Package for USG6525F),Per Device,1 Year