HUAWEI HiSecEngine USG6500F Series AI Firewalls

1 Overview

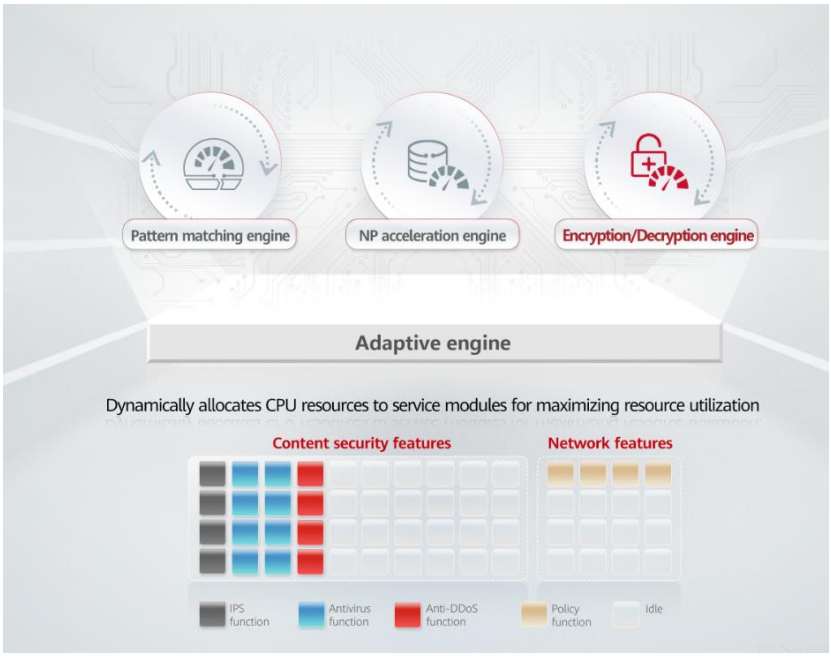
As digitalization is sweeping the world, extensive connections, explosive growth of data, and booming intelligent applications are profoundly changing the way we live and work. Enterprise services are going digital and moving to the cloud, which promotes the transformation of enterprise networks while 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 HiSecEngine USG6500F 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 USG6500F 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 USG6500F 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 USG6500F-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.

2 Product Highlights

Excellent performance

By leveraging fresh-new hardware and software architectures, 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 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.

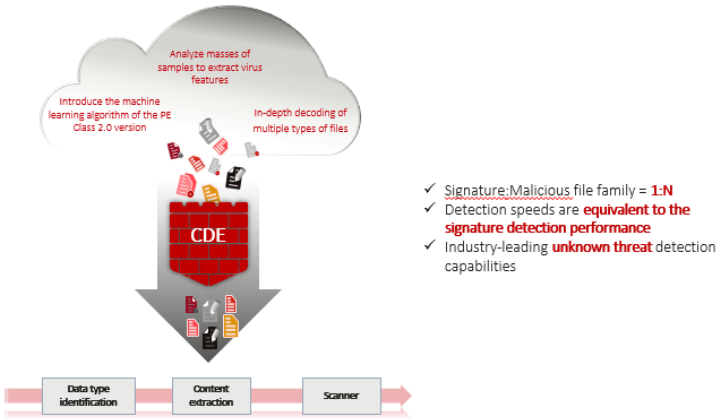


Intelligent defense

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.

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.



Simplified O&M

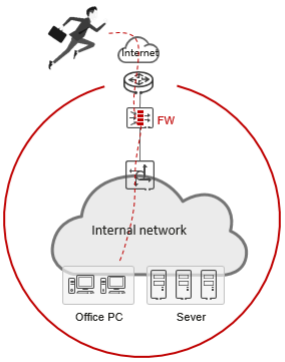
The HiSecEngine USG6500F series provides a brand-new web UI, which intuitively visualizes threats as well as displays key information such as device status, alarms, traffic, and threat events. With multi-dimensional data drilling, the web UI offers optimal user experience, enhanced usability, and simplified O&M.

The HiSecEngine USG6500F 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 HiSecEngine USG6500F 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.

3 Deployment

Small data center border protection

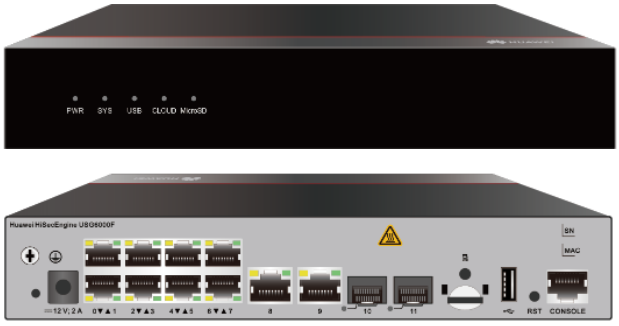
- Firewalls are deployed at egresses of data centers, and functions and system resources can be virtualized. The firewall has multiple types of interfaces, such as 10G (SFP+), GE (RJ45) and GE(SFP) interfaces. Services can be flexibly expanded without extra interface cards.
- The intrusion prevention 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.

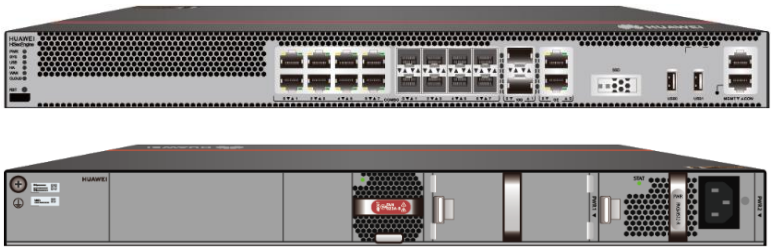
4 Product Appearance

Figure 4-1 HiSecEngine USG6510F-D/USG6530F-D



HiSecEngine USG6510F-DL/USG6530F-DL/ USG6510F-DPL/ USG6530F-DPL

HiSecEngine USG6525F/USG6555F/USG6565F/USG6585F



5 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.
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 13,000+ 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.

Feature	Description
URL filtering	Provides a URL category database with over 500 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.
Industrial control security	Supports management and control of 27 industrial control application protocols, such as Modbus, DNP3, IEC 60870-5-104, IEC 61850, OPC, S7, CIP, and PROFINET; supports intrusion detection and blocking for more than 100 industrial control systems: SCADA/Engineering/MES/HMI/PLC signature detection and blocking to reduce intrusion risks of known vulnerabilities. (The desktop model USG6500F-D/USG6500F-DL/USG6500F-DPL does not support industrial control security.)
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.
SSL offloading	Replaces servers to implement SSL encryption and decryption, effectively reducing server loads and implementing HTTP traffic load balancing. (Desktop model USG6500F-D/USG6500F-DL/USG6500F-DPL does not support SSL offloading.)
Anti-DDoS	Defends against more than 10 types of common DDoS attacks, including SYN flood and UDP flood attacks. (Note: Desktop models USG6500F-D, USG6500F-DL and USG6500F-DPL do not support the Anti-DDoS functions.)
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	Supports transparent, routing, and hybrid working modes and high availability

Feature	Description
reliability	(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.

6 Specifications

System Performance and Capacity

Model	USG6510F-D	USG6530F-D	USG6510F-DL USG6510F-DPL	USG6530F-DL USG6530F-DPL
IPv4 Firewall Throughput[1] (1518/512/64-byte, UDP)	2.5/2.5/2.5 Gbps	5/5/3.6 Gbps	2.5/2.5/2.5 Gbps	5/5/3.6 Gbps
IPv6 Firewall Throughput[1] (1518/512/84-byte, UDP)	2.5/2.5/2.5 Gbps	5/5/3.6 Gbps	2.5/2.5/2.5 Gbps	5/5/3.6 Gbps
Firewall Throughput (Packets Per Second)	3.75 Mpps	5.4 Mpps	3.75 Mpps	5.4 Mpps
Firewall Latency (64-byte, UDP)	18 us	18 us	18 us	18 us
FW + SA* Throughput[2]	1.8 Gbps	2.2 Gbps	1.8 Gbps	2.2 Gbps
NGFW Throughput (HTTP 100K)[3]	1.6 Gbps	1.8 Gbps	1.6 Gbps	1.8 Gbps
NGFW Throughput (Enterprise Mix) [4]	800 Mbps	900 Mbps	800 Mbps	900 Mbps
Threat Protection Throughput (HTTP 100K)[7]	1.3 Gbps	1.5 Gbps	1.3 Gbps	1.5 Gbps
Threat Protection Throughput (Enterprise Mix)[5]	700 Mbps	800 Mbps	700 Mbps	800 Mbps
Concurrent Sessions	300,000	500,000	300,000	500,000
IPv6 Concurrent Sessions[1]	200,000	500,000	200,000	500,000

Model	USG6510F-D	USG6530F-D	USG6510F-DL USG6510F-DPL	USG6530F-DL USG6530F-DPL
New Sessions/Second (HTTP1.1)[1]	20,000	30,000	20,000	30,000
IPv6 New Sessions/Second (HTTP1.1)[1]	8,000	30,000	8,000	30,000
IPsec VPN Throughput[1] (AES-256 + SHA256, 1420-byte)	2 Gbps	3.7 Gbps	2 Gbps	3.7 Gbps
Maximum IPSec VPN Tunnels (GW to GW)	1,000	2,000	1,000	2,000
Maximum IPsec VPN Tunnels (Client to GW)	1,000	2,000	1,000	2,000
SSL Inspection Throughput[8]	200 Mbps	300 Mbps	200 Mbps	300 Mbps
SSL VPN Throughput[6]	200 Mbps	300 Mbps	200 Mbps	300 Mbps
Concurrent SSL VPN Users (Default/Maximum)	100/100	100/1,000	100/100	100/1,000
Security Policies (Maximum)	3,000	3,000	3,000	3,000
Virtual Firewalls	10	20	10	20
URL Filtering: Categories	More than 130			
URL Filtering: URLs	A database of over 500 million URLs in the cloud			
Automated IPS Signature Updates	Yes, an industry-leading security center from Huawei (http://sec.huawei.com/sec/web/index.do)			
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
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	9/8/4 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	9/8/4 Gbps

Model	USG6525F	USG6555F	USG6565F	USG6585F
Firewall Throughput (Packets Per Second)	3.75 Mpps	5.4 Mpps	5.4 Mpps	6 Mpps
Firewall Latency (64-byte, UDP)	18 us	18 us	18 us	18 us
FW + SA* Throughput[2]	2.2 Gbps	2.5 Gbps	3 Gbps	3 Gbps
NGFW Throughput (HTTP 100K)[3]	1.8 Gbps	2.1 Gbps	2.2 Gbps	2.2 Gbps
NGFW Throughput (Enterprise Mix) [4]	1 Gbps	1.1 Gbps	1.2 Gbps	1.3 Gbps
Threat Protection Throughput (HTTP 100K)[7]	1.5 Gbps	1.8 Gbps	2 Gbps	2 Gbps
Threat Protection Throughput (Enterprise Mix)[5]	900 Mbps	1 Gbps	1.1 Gbps	1.2 Gbps
Concurrent Sessions	3,000,000	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
New Sessions/Second (HTTP1.1)[1]	80,000	80,000	80,000	80,000
IPv6 New Sessions/Second (HTTP1.1)[1]	80,000	80,000	80,000	80,000
IPsec VPN Throughput[1] (AES-256 + SHA256, 1420-byte)	2.1 Gbps	3.7 Gbps	3.7 Gbps	3.7 Gbps
Maximum IPSec VPN Tunnels (GW to GW)	4,000	4,000	4,000	4,000
Maximum IPsec VPN Tunnels (Client to GW)	4,000	4,000	4,000	4,000
SSL Inspection Throughput[8]	300 Mbps	450 Mbps	500 Mbps	550 Mbps
SSL VPN Throughput[6]	300 Mbps	500 Mbps	500 Mbps	500 Mbps
Concurrent SSL VPN Users (Default/Maximum)	100/1,000	100/2,000	100/2,000	100/2,000
Security Policies (Maximum)	15,000	15,000	15,000	15,000
Virtual Firewalls	100	100	100	100
URL Filtering: Categories	More than 130			
URL Filtering: URLs	A database of over 500 million URLs in the cloud			

Model	USG6525F	USG6555F	USG6565F	USG6585F
Automated IPS Signature Updates	Yes, an industry-leading security center from Huawei (http://sec.huawei.com/sec/web/index.do)			
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. 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.

7 Hardware Specifications

Model	USG6510F-D	USG6530F-D	USG6510F-DL USG6510F-DPL	USG6530F-DL USG6530F-DPL
Dimensions (W x D x H) mm	250 x 210 x 43.6		320 x 220 x 43.6	
Form Factor/Height	Desktop			
Fixed Interface	10*GE RJ45 + 2*GE SFP	10*GE RJ45 + 2*10GE SFP+	4*GE SFP + 8*GE RJ45 + LTE	2*10GE SFP+ + 2*GE SFP + 8*GE RJ45 + LTE
USB Port	1 x USB 2.0			
Weight	1.55 kg		2.34 kg	
External Storage	Optional, 64 GB microSD card available for purchase			

Model	USG6510F-D	USG6530F-D	USG6510F-DL USG6510F-DPL	USG6530F-DL USG6530F-DPL
Power Supply	100 V to 240 V, 50 Hz/60 Hz			
Maximum power consumption of the machine	36 W		46.5 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	USG6525F	USG6555F	USG6565F	USG6585F
Dimensions (W x D x H) mm	442 × 420 × 43.6			
Form Factor/Height	1 U			
Fixed Interface	2*GE RJ45 + 8*GE COMBO + 2*10GE SFP+			
USB Port	2 x USB 2.0			
Weight	5.46 kg			
External Storage	Optional, M.2 SSD (64 GB/240 GB), hot-swappable			
Power Supply	100 V to 240 V, 50 Hz/60 Hz			
Maximum power consumption of the machine	49.5 W			
Power Supplies	Optional dual power modules for 1+1 redundancy			
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			

8 Ordering Information

Product	Model	Description
USG6510F-D	USG6510F-D-AC	USG6510F-D AC host (10*GE RJ45+2*GE SFP,1*Adapter)
USG6530F-D	USG6530F-D-AC	USG6530F-D AC host (10*GE RJ45 + 2*10GE SFP+,1*Adapter)
USG6510F-DL	USG6510F-DL-AC	USG6510F-DL AC host (4*GE SFP + 8*GE RJ45 + LTE,1*Adapter)
USG6530F-DL	USG6530F-DL-AC	USG6530F-DL AC host (2*10GE SFP+ + 2*GE SFP + 8*GE RJ45 + LTE,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, Maximum power supply capability:150W.
USG6530F-DPL	USG6530F-DPL-AC	USG6530F-DPL AC Host(2*10GE SFP+ +2*GE SFP+8*GE RJ45+ LTE, 1*Adapter, include SSL VPN 100 users) Supports 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+)
USG6555F	USG6555F-AC	USG6555F AC host (2*GE RJ45 + 8*GE COMBO + 2*10GE SFP+,1 AC power)
USG6565F	USG6565F-AC	USG6565F AC host (2*GE RJ45 + 8*GE COMBO + 2*10GE SFP+,1 AC power)
	USG6565F-DC	USG6565F DC host (2*GE RJ45 + 8*GE COMBO + 2*10GE SFP+)
USG6585F	USG6585F-AC	USG6585F AC host (2*GE RJ45 + 8*GE COMBO + 2*10GE SFP+,1 AC power)
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)
NGFW License		
IPS Update Service	LIC-USG6525F-IPS-1Y	IPS Update Service Subscribe Per Year (Applies to USG6525F)

Product	Model	Description
	LIC-USG6555F-IPS-1Y	IPS Update Service Subscribe Per Year (Applies to USG6555F)
	LIC-USG6565F-IPS-1Y	IPS Update Service Subscribe Per Year (Applies to USG6565F)
	LIC-USG6585F-IPS-1Y	IPS Update Service Subscribe Per Year (Applies to USG6585F)
	LIC-USG6510F-DPL-IPS-1Y	IPS Update Service Subscribe Per Year (Applies to USG6510F-DPL)
	LIC-USG6530F-DPL-IPS-1Y	IPS Update Service Subscribe Per Year (Applies to USG6530F-DPL)
URL Filtering Update Service	LIC-USG6525F-URL-1Y	URL Update Service Subscribe Per Year (Applies to USG6525F)
	LIC-USG6555F-URL-1Y	URL Update Service Subscribe Per Year (Applies to USG6555F)
	LIC-USG6565F-URL-1Y	URL Update Service Subscribe Per Year (Applies to USG6565F)
	LIC-USG6585F-URL-1Y	URL Update Service Subscribe Per Year (Applies to USG6585F)
	LIC-USG6510F-DPL-URL-1Y	URL Update Service Subscribe Per Year (Applies to USG6510F-DPL)
	LIC-USG6530F-DPL-URL-1Y	URL Update Service Subscribe Per Year (Applies to USG6530F-DPL)
Antivirus Update Service	LIC-USG6525F-AV-1Y	AV Update Service Subscribe Per Year (Applies to USG6525F)
	LIC-USG6555F-AV-1Y	AV Update Service Subscribe Per Year (Applies to USG6555F)
	LIC-USG6565F-AV-1Y	AV Update Service Subscribe Per Year (Applies to USG6565F)
	LIC-USG6585F-AV-1Y	AV Update Service Subscribe Per Year (Applies to USG6585F)
	LIC-USG6510F-DPL-AV-1Y	AV Update Service Subscribe Per Year (Applies to USG6510F-DPL)
	LIC-USG6530F-DPL-AV-1Y	AV Update Service Subscribe Per Year (Applies to USG6530F-DPL)
Threat Protection Bundle (IPS, AV, URL)	LIC- USG6510F-D -TP-1Y	Threat Protection Subscription Per Year (Applies to USG6510F-D Overseas)
	LIC-USG6530F-D-TP-1Y	Threat Protection Subscription Per Year (Applies to USG6530F-D Overseas)

Product	Model	Description
	LIC-USG6510F-DL-TP-1Y	Threat Protection Subscription Per Year (Applies to USG6510F-DL Overseas)
	LIC-USG6530F-DL-TP-1Y	Threat Protection Subscription Per Year (Applies to USG6530F-DL Overseas)
	LIC-USG6510F-DPL-TPU-1Y	Threat Protection Database Upgrade Service (Applies to USG6510F-D), Per Device, Per Year
	LIC-USG6530F-DPL-TP-1Y	Threat Protection Subscription Per Year (Applies to USG6530F-DPL)
	LIC-USG6525F-TP-1Y	Threat Protection Subscription Per Year (Applies to USG6525F Overseas)
	LIC-USG6555F-TP-1Y	Threat Protection Subscription Per Year (Applies to USG6555F Overseas)
	LIC-USG6565F-TP-1Y	Threat Protection Subscription Per Year (Applies to USG6565F Overseas)
	LIC-USG6585F-TP-1Y	Threat Protection Subscription Per Year (Applies to USG6585F Overseas)
IPv6+	N1-AD-USG6500F-IPv6+-LIC	IPv6+ Feature (includes SRv6,channel subinterface, iFit) (Applies to USG6500F)
Industrial Control Security Service	LIC-USG6525F-ICS-1Y	Industrial Control Security Service Subscribe Per Year (Applies to USG6525F)
	LIC-USG6555F-ICS-1Y	Industrial Control Security Service Subscribe Per Year (Applies to USG6555F)
	LIC-USG6565F-ICS-1Y	Industrial Control Security Service Subscribe Per Year (Applies to USG6565F)
	LIC-USG6585F-ICS-1Y	Industrial Control Security Service Subscribe Per Year (Applies to USG6585F)
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
USG6530F-D	N1-USG6530F-D-F-Lic	N1-USG6530F-D Foundation, Per Device
	N1-USG6530F-D-F-SnS1Y	N1-USG6530F-D Foundation, SnS, Per Device, Per Year
USG6510F-DL	N1-USG6510F-DL-F-Lic	N1-USG6510F-DL Foundation, Per Device
	N1-USG6510F-DL-F-SnS1Y	N1-USG6510F-DL Foundation, SnS, Per Device, Per Year
USG6530F-DL	N1-USG6530F-DL-F-Lic	N1-USG6530F-DL Foundation, Per Device
	N1-USG6530F-DL-F-SnS1Y	N1-USG6530F-DL Foundation, SnS, Per Device, Per Year

Product	Model	Description
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
USG6530F-DPL	N1-USG6530F-DPL-F-Lic	N1-USG6530F-DPL Foundation, Per Device
	N1-USG6530F-DPL-A-Lic	N1-USG6530F-DPL Advanced, Per Device
	N1-USG6530F-DPL-F-SnS1AY	N1-USG6530F-DPL Foundation, SnS, Per Device, Per Year
	N1-USG6530F-DPL-A-SnS1AY	N1-USG6530F-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
USG6555F	N1-USG6555F-F-Lic	N1-USG6555F Foundation, Per Device
	N1-USG6555F-F-SnS1Y	N1-USG6555F Foundation, SnS, Per Device, Per Year
	N1-USG6555F-A-Lic	N1-USG6555F Advanced, Per Device
	N1-USG6555F-A-SnS1Y	N1-USG6555F Advanced, SnS, Per Device, Per Year
USG6565F	N1-USG6565F-F-Lic	N1-USG6565F Foundation, Per Device
	N1-USG6565F-F-SnS1Y	N1-USG6565F Foundation, SnS, Per Device, Per Year
	N1-USG6565F-A-Lic	N1-USG6565F Advanced, Per Device
	N1-USG6565F-A-SnS1Y	N1-USG6565F Advanced, SnS, Per Device, Per Year
USG6585F	N1-USG6585F-F-Lic	N1-USG6585F Foundation, Per Device
	N1-USG6585F-F-SnS1Y	N1-USG6585F Foundation, SnS, Per Device, Per Year
	N1-USG6585F-A-Lic	N1-USG6585F Advanced, Per Device
	N1-USG6585F-A-SnS1Y	N1-USG6585F Advanced, SnS, Per Device, Per Year

NOTE

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

About This Publication

This publication is for reference only and shall not constitute any commitments or guarantees. All trademarks, pictures, logos, and brands mentioned in this document are the property of Huawei Technologies Co., Ltd. or a third party.

For more information, visit http://e.huawei.com/en/products/enterprise-networking/security.