HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls

1 Overview

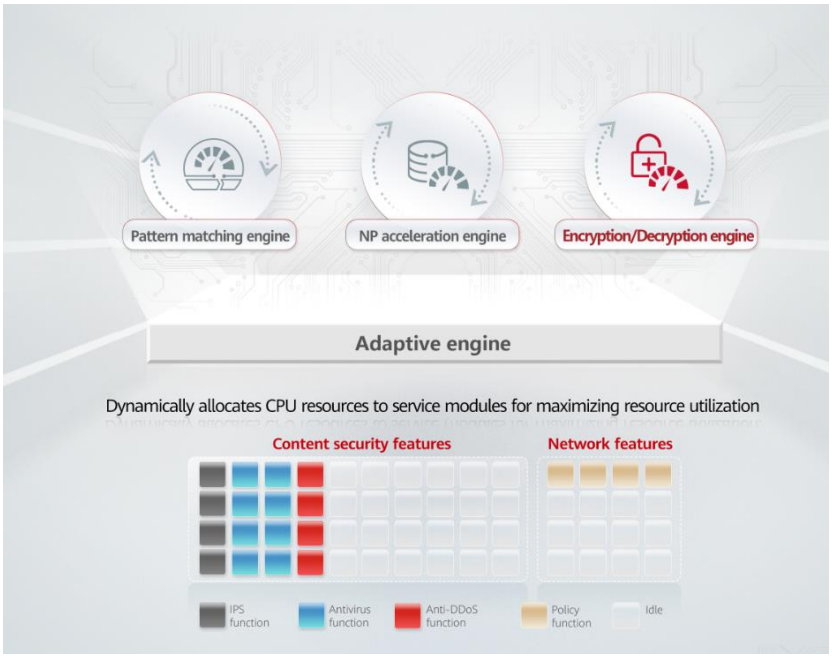
As digitalization is sweeping the world, extensive connections, explosive growth of data, and booming intelligent applications are profoundly changing the way we live and work. Enterprise services are going digital and moving to the cloud, which promotes the transformation of enterprise networks while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

2 Product Highlights

Excellent performance

By leveraging fresh-new hardware and software architectures, HiSecEngine USG6000F series AI firewalls dynamically allocate resources to service modules through the adaptive security engine (ASE), maximizing resource utilization and improving overall service performance. For core services, the HiSecEngine USG6000F 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.



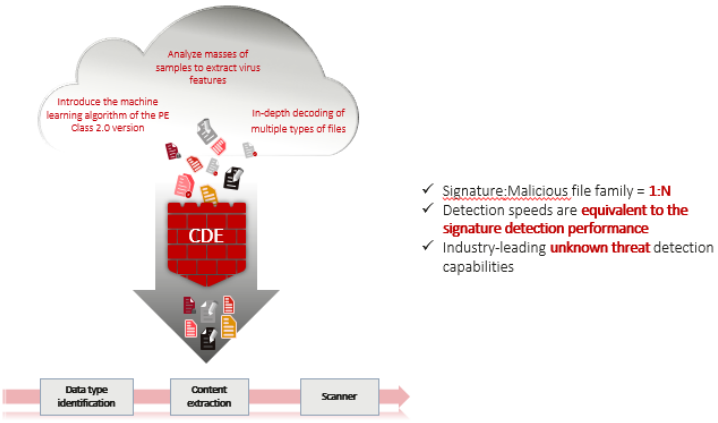
Intelligent defense

HiSecEngine USG6000F 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.

NGFW USG 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 HiSecEngine USG6000F 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.

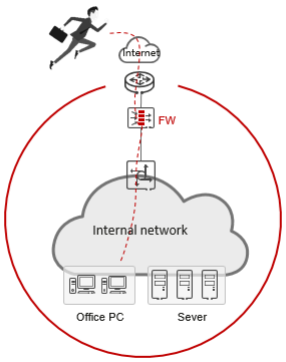
The HiSecEngine USG6000F series firewalls can be centrally managed by the security management platform SecoManager, implementing a shift from single-point defense to collaborative network protection. The SecoManager provides policy tuning and intelligent O&M capabilities. It can also manage security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

The HiSecEngine USG6000F series NGFW 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 USG6000F series also provides various network features such as VPN, IPv6, and intelligent traffic steering.

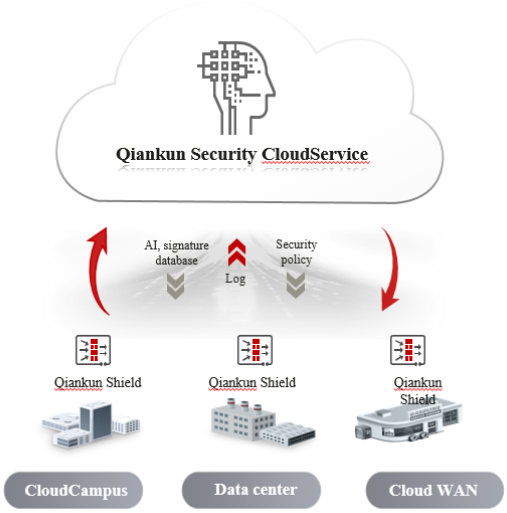
- Provides various VPN features such as IPsec VPN and SSL VPN, and supports multiple encryption algorithms, such as DES, 3DES, AES, and SHA, ensuring secure and reliable data transmission.



- 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.

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 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.



Precise detection

- IPS/Anti-virus detection : real-time detection and blocking by Qiankun Shield, 22000+ IPS signature database, default blocking rate of up to 85%

Automatic analysis

- AI analysis : intelligent aggregation and analysis of massive logs based on 10+ expert models on the cloud, and identifies threats in seconds

Fast closed-loop handling

- Correlation analysis for source tracing: cloud-based multi-dimensional correlation analysis of threat intelligence, and implementing precise attack source tracing
- Automatic closed-loop handling: real-time alarms about compromised hosts, external attack source blocking in minutes, with an overall automatic handling rate of 96%

Optimal experience

- Periodic security reports: automatically sending weekly and monthly reports to users
- Emergency notification: risk notifications to users through SMS, email
- Visualized management : real-time security situation dashboard

- 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.

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 100G,40G, 10G, and 1G 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 USG6615F/USG6625F

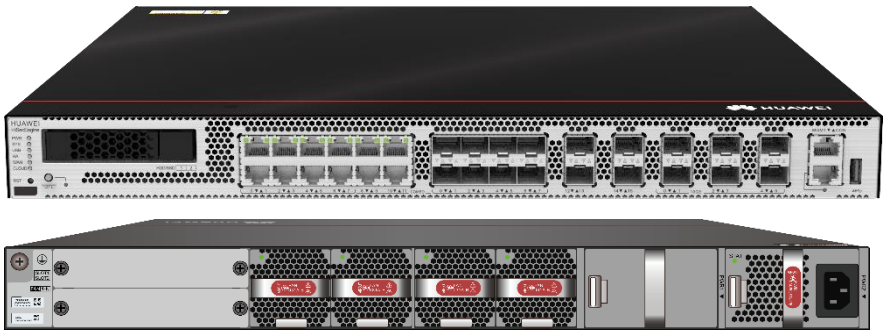


Figure 4-2 HiSecEngine USG6635F/USG6655F/USG6685F



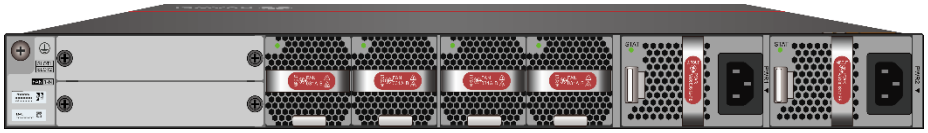


Figure 4-3 HiSecEngine USG6710F/USG6715F

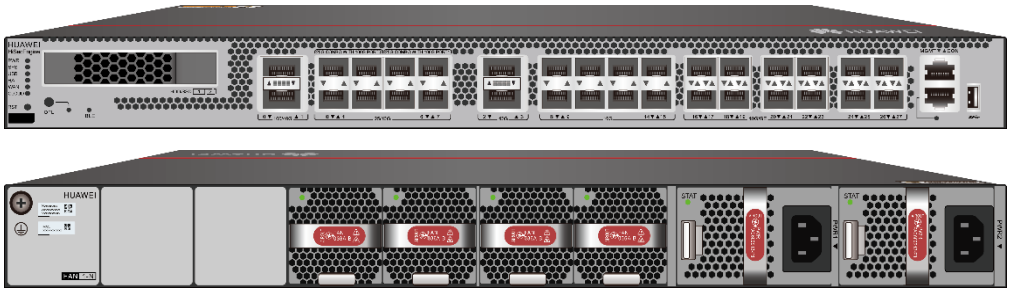
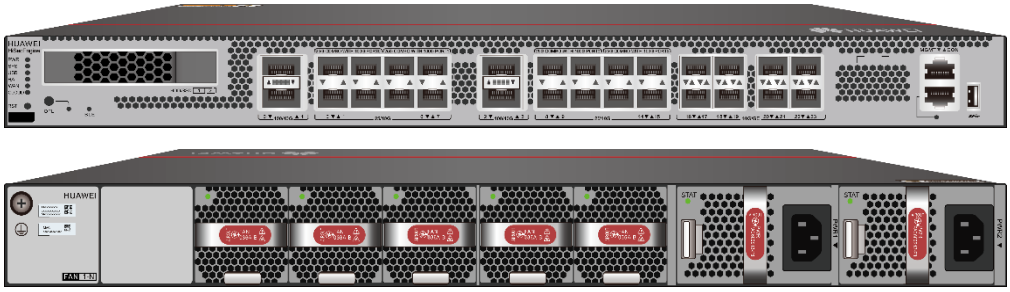


Figure 4-4 HiSecEngine USG6725F



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 6000 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),

Feature	Description
	botnets ,remote control, and Trojan horses, and supports brute-force attack detection. Supports 22,000+ 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. Supports intelligent, heuristic antivirus engine that can detect hundreds of millions of virus variants. Supports virus detection for files using protocols such as HTTP/FTP/SMTP/POP3/IMAP4/NFS/SMB. Detects Trojan horses, worms, spyware, vulnerability exploit programs, adware, hacker tools, rootkits, backdoors, grayware, botnet programs, ransomware, phishing software, mining software, and web shell programs. Supports virus detection for various file types, such as Office documents, executable files (Windows/Linux/MacOS), script files, Flash files, PDF files, RTF files, web pages, and images. Supports attack evidence collection. Supports virus detection for a maximum of 100 layers of compressed files, including tar, gzip, zip, rar, and 7z files.
Bandwidth management	Manages per-user and per-IP bandwidth based on service application identification, ensuring the network experience of key services and users. The management and control can be implemented by limiting the maximum bandwidth, guaranteeing the minimum bandwidth, and changing the application forwarding priority.
URL filtering	Provides a URL category database with over 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.
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

Feature	Description
	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.
Anti-DDoS	Defends against over 20 types of single-packet attacks and over 10 types of DDoS attacks, such as SYN flood, UDP flood, ICMP flood, HTTP flood, HTTPS flood, DNS flood, and SIP flood.
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. Provides security policy management solutions in partnership with Firemon and AlgoSec to reduce O&M costs and potential faults.
Routing	Supports multiple types of routing protocols and features, such as RIP, OSPF, BGP, IS-IS, RIPng, OSPFv3, BGP4+, and IPv6 IS-IS.
SRv6	IS-IS for SRv6、 SRv6 TE Policy、 SRv6 SRH compressing SRv6 BGP、 SRv6 BE、 SRv6 BE SBFD、 SRv6 TI-LFA FRR、 SRv6 intermediate node protection、 SRv6 Anti-Micro-Ring、 SRv6 OAM、 EVPN L3VPN
Secure SD-WAN	Built-in secure SD-WAN solution to build low-cost, business-grade Internet links ZTP one-click deployment (email), zero skill requirements, and device provisioning in minutes FEC is supported. No artifact or frame freezing occurs when the video packet loss rate reaches 30%. Link selection based on link quality and real-time link switchover ensure the experience of key applications. Multi-link routing and dual-CPE flexible networking ensure that site services are not interrupted. End-to-end IPSec encryption, secure and reliable devices, and secure service transmission. The USG6600F series can be a spoke or a hub,USG6700F series doesn’t support SD-WAN

Feature	Description
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.
IP multicast	Supports IPv4 Layer 3 multicast protocols, such as IGMP, MSDP, PIM, and provides point-to-multipoint services to reduce bandwidth consumption.
Deployment and reliability	Supports transparent, routing, and hybrid working modes and high availability (HA), including the Active/Active and Active/Standby modes.
Server load balancing	Supports IPv6, L4/L7 server load balancing, and multiple session persistence methods based on source IP addresses and HTTP cookies; supports SSL offloading and encryption; supports combination of services and security policies for effective service security enhancement; supports health check based on multiple protocols, such as TCP, RADIUS, DNS, and HTTP, to detect server status changes in a timely manner.
Asset management	Provides asset-based threat visualization, which supports associating IPS and Antivirus threat logs with user assets and displaying asset risk assessment results.
PPPoE	Functions as a PPPoE client to provide Internet access services, including user authentication and authorization and dynamic IP address allocation.
Behavior and content	Audits and traces the sources of the accessed content based on users
User authentication	Supports multiple user authentication methods, including local, RADIUS, HWTACACS, AD, and LDAP. The firewall supports built-in Portal and Portal redirection functions,It can synchronize the users that go online from the RADIUS server or Agile Controller (NCE-Campus) to the device.

6 Specifications

System Performance and Capacity

Model	USG6615F	USG6625F	USG6635F	USG6655F
IPv4Firewall Throughput[1] (1518/512/64-byte, UDP)	15/15/15 Gbps	25 /25 /25 Gbps	35/35/35 Gbps	50/50/40 Gbps
IPv6 Firewall Throughput1 (1518/512/84-byte, UDP)	15/15/15 Gbps	25 /25 /25 Gbps	35/35/25 Gbps	50/50/25 Gbps

Model	USG6615F	USG6625F	USG6635F	USG6655F
Secure SD-WAN EVPN Throughput(1400/512 byte,UDP) [9]	15/15 Gbps	25 /25 Gbps	35/35 Gbps	50/40 Gbps
Secure SD-WAN EVPN tunnels	3,000	3,000	6,000	6,000
Firewall Latency (64-byte, UDP)	18μs	18 μs	18 μs	18 μs
Concurrent Sessions (HTTP1.1)[1]	10,000,000	10,000,000	20,000,000	20,000,000
New Sessions/Second (HTTP1.1)[1]	250,000	250,000	500,000	500,000
FW + SA* Throughput[2]	12Gbps	12Gbps	23Gbps	26.5Gbps
NGFW Throughput[3] (HTTP 100K)	6Gbps	10Gbps	16Gbps	25Gbps
NGFW Throughput (Enterprise Mix)[4]	4.6Gbps	5Gbps	8Gbps	8.5Gbps
Threat Protection Throughput (Enterprise Mix)[5]	4Gbps	4Gbps	7Gbps	8Gbps
IPsec VPN Throughput[1] (AES-256 + SHA256, 1420-byte)	15Gbps	25Gbps	30Gbps	30Gbps
Maximum IPsec VPN Tunnels	15,000	15,000	20,000	20,000
SSL Inspection Throughput[7]	2.5 Gbps	2.5 Gbps	4 Gbps	4 Gbps
SSL VPN Throughput [6]	1 Gbps	1.5 Gbps	3 Gbps	3 Gbps
Concurrent SSL VPN Users *(Default/Maximum)	100/4000	100/8000	100/10000	100/10000
Security Policies (Maximum)	50,000	50,000	100,000	100,000
Virtual Firewalls	2048	2048	2048	2048
URL Filtering: Categories	More than 130			
URL Filtering: URLs	A database of over 500 million URLs in the cloud			

Model	USG6615F	USG6625F	USG6635F	USG6655F
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	USG6685F	USG6710F	USG6715F	USG6725F
IPv4Firewall Throughput[1] (1518/512/64-byte, UDP)	80/80/40 Gbps	100/100/60 Gbps	160/160/80 Gbps	240/240/120 Gbps
IPv6 Firewall Throughput1 (1518/512/84-byte, UDP)	80/80/25 Gbps	100/100/45 Gbps	160/160/50 Gbps	240/240/85 Gbps
Secure SD-WAN EVPN Throughput(1400/512 byte,UDP) [9]	50/40 Gbps	/	/	/
Secure SD-WAN EVPN tunnels	6000	/	/	/
Firewall Latency (64-byte, UDP)	18 μs	35 μs	35 μs	35 μs
Concurrent Sessions (HTTP1.1)[1]	25,000,000	30,000,000	50,000,000	75,000,000
New Sessions/Second (HTTP1.1)[1]	750,000	1,000,000	1,500,000	2,250,000
FW + SA* Throughput[2]	26.5Gbps	50Gbps	55Gbps	80Gbps
NGFW Throughput[3]	25Gbps	40Gbps	50Gbps	75Gbps
NGFW Throughput (Enterprise Mix)[4]	8.5Gbps	16Gbps	17Gbps	26Gbps
Threat Protection Throughput (Enterprise Mix)[5]	8Gbps	14Gbps	16Gbps	24Gbps

Model	USG6685F	USG6710F	USG6715F	USG6725F
IPsec VPN Throughput[1] (AES-256 + SHA256, 1420-byte)	30Gbps	40Gbps	45Gbps	65 Gbps
Maximum IPsec VPN Tunnels	20000	40000	40000	60000
SSL Inspection Throughput[7]	4 Gbps	8 Gbps	8 Gbps	12 Gbps
SSL VPN Throughput[6]	5 Gbps	10 Gbps	10 Gbps	12 Gbps
Concurrent SSL VPN Users *(Default/Maximum)	100/10000	100/20000	100/20000	100/30000
Security Policies (Maximum)	100,000	100,000	100,000	100,000
Virtual Firewalls	2048	2048	2048	2048
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			

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. SSL inspection throughput is measured with IPS-enabled and HTTPS traffic using TLS v1.2 with TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256.
8. The data test condition is the interface pair mode.
9. The SD-WAN tunnel is packed with GRE over IPSec.

*SA: indicates service awareness.

7 Hardware Specifications

Model	USG6615F	USG6625F	USG6635F	USG6655F
Chassis Height	1 U			
Dimensions (H x W x D) mm	43.6 x 442 x 420			
Fixed Interface	8*GE COMBO + 4*GE RJ45 + 4*GE SFP + 6*10GE SFP+		8*GE COMBO + 4*GE RJ45 + 10*10GE SFP+	
USB Port	1 x USB 3.0			
Weight	6.3 kg	7.3 kg		
Hardware	Optional, SATA (1 x 2.5 inch) supported, 240GB/480GB/960GB/1920GB, hot-swappable			
Power Supply(AC)	100 V to 240 V			
Maximum power consumption of the machine	222 W		242 W	
Power Supplies	Optional dual AC power supplies		Dual AC 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	USG6685F	USG6710F	USG6715F	USG6725F
Chassis Height	1 U			
Dimensions (H x W x D) mm	43.6 x 442 x 420			
Fixed Interface	8*GE COMBO + 4*GE(RJ45)+ 10*10GE(SFP+)	2*100GE(QSFP28) + 2*40G(QSFP+)+ 8*25(ZSFP+) +		4*100GE(QSFP28) + 16*25GE(ZSFP+)

Model	USG6685F	USG6710F	USG6715F	USG6725F
		20*10GE(SFP+)[1]		+ 8*10GE(SFP+)[2]
USB Port	1 x USB 3.0			
Weight	7.3 kg	10.26 kg		10.6 kg
External Storage	Optional, SATA (1 x 2.5 inch) supported, 240GB/480GB/960GB /1920GB			
Power Supply	100 V to 240 V			
Maximum power consumption of the machine	242 W	391 W		445 W
Power Supplies	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			

1. *Some 100GE interfaces and 25GE interfaces of USG6710F and USG6715F are mutually exclusive.*
2. *Some 100GE interfaces and 25GE interfaces of USG6715F are mutually exclusive.*

8 Ordering Information

Note:

1、The ordering information of USG6625F/USG6635F/USG6655F/USG6685F is the same of 2、USG6615F

2、The ordering information of USG6710F/USG6715F is the same as USG6725F

3、The model USG6615F support Qiankun Security Cloud Service

Product	Model	Description
USG6615F	USG6615F-AC	USG6615F AC Host (8*GE COMBO + 4*GE RJ45 + 4*GE SFP + 6*10GE SFP+, 1 AC power supply)
USG6725F	USG6725F-AC	USG6725F AC Host (4*QSFP28 + 16*ZSFP+ + 8*SFP+,,2 AC power supplies)
Function License		
Virtual Firewall	LIC-USG6KF-VSYS-10	Quantity of Virtual Firewall (10 Vsys)
	LIC-USG6KF-VSYS-20	Quantity of Virtual Firewall (20 Vsys)

Product	Model	Description
	LIC-USG6KF-VSYS-50	Quantity of Virtual Firewall (50 Vsys)
	LIC-USG6KF-VSYS-100	Quantity of Virtual Firewall (100 Vsys)
	LIC-USG6KF-VSYS-200	Quantity of Virtual Firewall (200 Vsys)
	LIC-USG6KF-VSYS-500	Quantity of Virtual Firewall (500 Vsys)
	LIC-USG6KF-VSYS-1000	Quantity of Virtual Firewall (1000 Vsys)
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-USG6615F-IPS-1Y	IPS Update Service Subscribe Per Year (Applies to USG6615F)
	LIC-USG6725F-IPS-1Y	IPS Update Service Subscribe Per Year (Applies to USG6725F)
URL Filtering Update Service	LIC-USG6615F-URL-1Y	URL Update Service Subscribe Per Year (Applies to USG6615F)
	LIC-USG6725F-URL-1Y	URL Update Service Subscribe Per Year (Applies to USG6725F)
Antivirus Update Service	LIC-USG6615F-AV-1Y	AV Update Service Subscribe Per Year (Applies to USG6615F)
	LIC-USG6725F-AV-1Y	AV Update Service Subscribe Per Year (Applies to USG6725F)
Threat Protection Bundle (IPS, AV, URL)	LIC-USG6615F-TP -1Y-OVS	Threat Protection Subscription Per Year (Applies to USG6615F Overseas)
	LIC-USG6725F-TP-1Y-OVS	Threat Protection Subscription Per Year

Product	Model	Description
		(Applies to USG6725F Overseas)
Industrial Control Security Service	LIC-USG6615F-ICS-1Y	Industrial Control Security Service Subscribe Per Year (Applies to USG6615F)
	LIC-USG6725F-ICS-1Y	Industrial Control Security Service Subscribe Per Year (Applies to USG6725F)
IPv6+	N1-AD-USG6600F-IPv6+-LIC	IPv6+ Feature (includes SRv6,channel subinterface, iFit) (Applies to USG6600F)
	N1-AD-USG6700F-IPv6+-LIC	IPv6+ Feature (includes SRv6,channel subinterface, iFit) (Applies to USG6700F)
Enhanced DDoS defense	LIC-USG6000F-AntiDDoS	Enhanced anti-DDoS function (applies to USG6000F)
N1 License		
USG6615F	N1-USG6615F-F-Lic	N1-USG6615F Foundation, Per Device
	N1-USG6615F-F-SnS1Y	N1-USG6615F Foundation, SnS, Per Device, Per Year
	N1-USG6615F-A-Lic	N1-USG6615F Advanced, Per Device
	N1-USG6615F-A-SnS1Y	N1-USG6615F Advanced, SnS, Per Device, Per Year
USG6725F	N1-USG6725F-F-Lic	N1-USG6725F Foundation, Per Device
	N1-USG6725F-F-SnS1Y	N1-USG6725F Foundation, SnS, Per Device, Per Year
	N1-USG6725F-A-Lic	N1-USG6725F Advanced, Per Device
	N1-USG6725F-A-SnS1Y	N1-USG6725F Advanced, SnS, Per Device, Per Year
QianKun Cloud Deployment License		
USG6615F	N1-C-USG6615F-F-Lic	Cloud Deployment Model Foundation, Per Device,Per Year
	LIC-USG6615F-BA-1Y	Border Protection and Response - Threat automatic blocking (Applies to USG6615F), Per Device, Per Year
	LIC-USG6615F-TPU-1Y	Threat Protection Database Upgrade Service (Applies to USG6510F-D), Per Device, Per Year
QianKun OP mode		

Product	Model	Description
USG6615F	LIC-USG6615F-TPU-1Y	Threat Protection Database Upgrade Service (Applies to USG6510F-D), Per Device, Per Year
N1 SASE Branch Interconnection license		
USG6615F	N1-USG6615F-S-S-Lic	N1 SASE Branch Interconnection Standard Package(Package for USG6615F)
	N1-USG6615F-S-S-S1Y	N1 SASE Branch Interconnection Standard Package(Package for USG6615F),Per Device,1 Year

NOTE

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