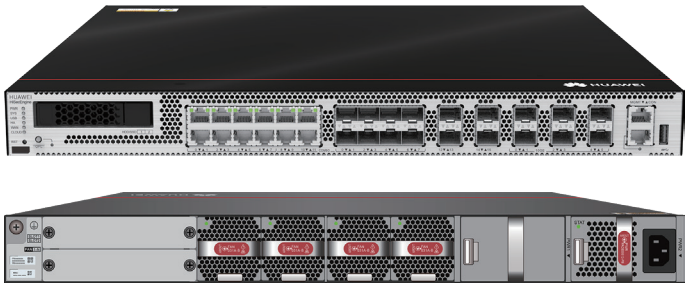
HUAWEI HiSecEngine USG6000F Series AI Firewalls (Fixed-Configuration)

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.

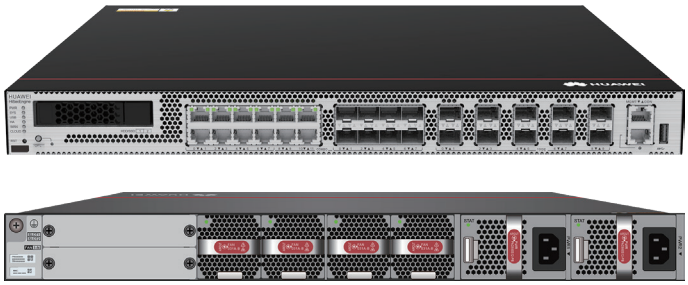
With new hardware and software architectures, Huawei HiSecEngine USG6000F series are next-generation AI firewalls that feature intelligent defense, outstanding performance, and simplified O&M, effectively addressing the preceding challenges. The USG6000F series uses intelligence technologies to enable 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, IPS devices, and anti-DDoS devices, reducing security O&M OPEX.

HUAWEI

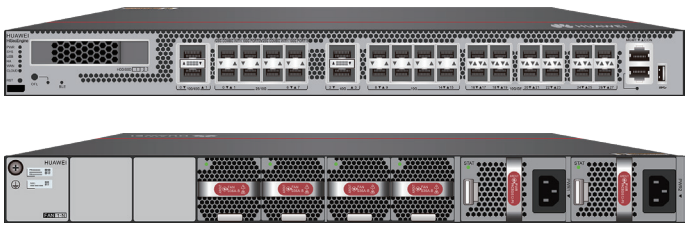
Product Appearance



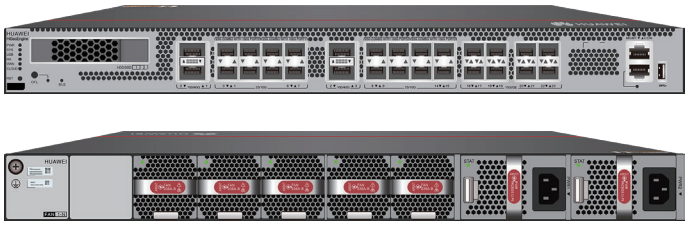
HiSecEngine USG6615F/USG6625F



HiSecEngine USG6635F/USG6655F/USG6685F



HiSecEngine USG6710F/USG6715F

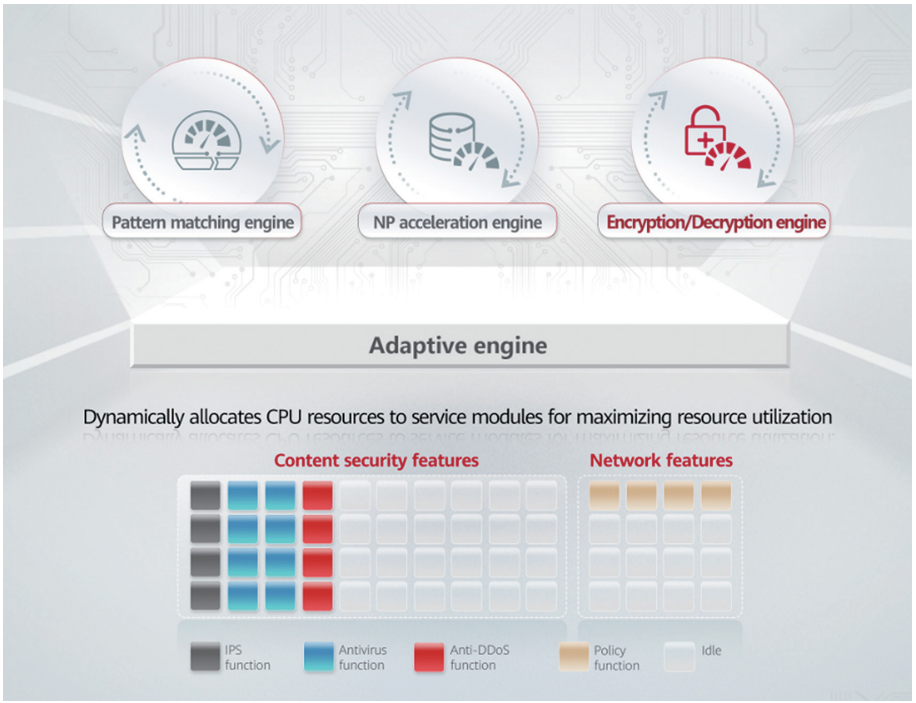


HiSecEngine USG6725F

Product Highlights

Excellent performance

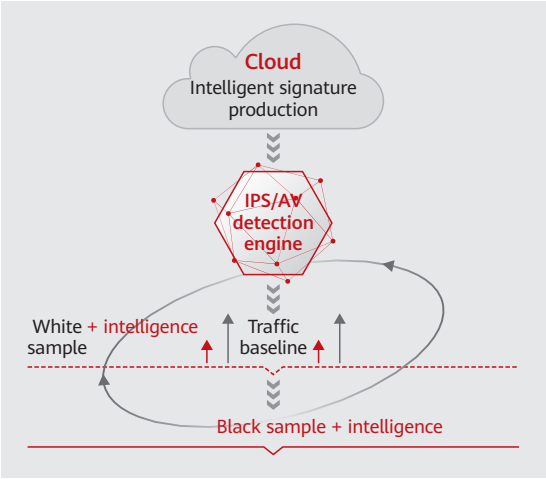
By leveraging fresh-new hardware and software architectures, HiSecEngine USG6000F series AI firewalls dynamically allocate resources to service modules through the adaptive security engine (ASE), maximizing resource utilization and improving overall service performance. For core services, the HiSecEngine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

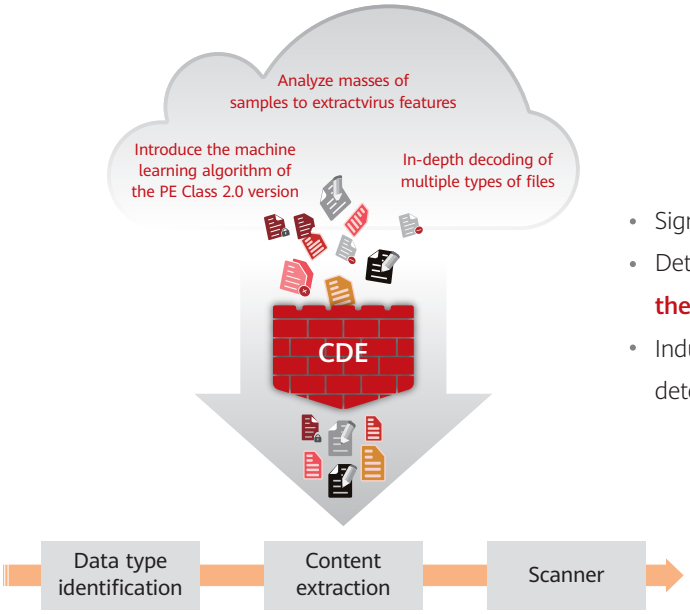
HiSecEngine USG6000F series AI firewalls provide content security functions, such as application identification, IPS, antivirus, and URL filtering to protect intranet servers and users against threats.

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.



- Intelligent signature production on the cloud, 30X increase in signature productivity
- Local baseline learning improves the IPS blocking accuracy
- Incremental learning of black samples and reverse training of the detection engine

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



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

Simplified O&M

The 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.

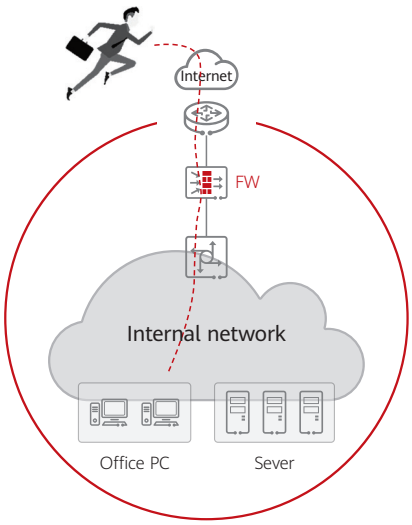
The HiSecEngine USG6000F series firewalls can be centrally managed by the security management platform SecoManager, implementing a shift from single-point defense to collaborative network

protection. The SecoManager provides policy tuning and intelligent O&M capabilities. It can also manage security products, such as IPS and anti-DDoS devices to quickly eliminate network threats and improve security handling effectiveness.

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.

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 40G, 10G, and 1G interfaces. Services can be flexibly expanded without extra interface cards.
- The 12-Gigabit 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 deception function is enabled on the firewalls to proactively respond to malicious scanning behavior, protecting enterprises against threats in real time.
- The policy control, data filtering, and audit functions of the firewalls are used to monitor social network applications to prevent data breach and protect enterprise networks.

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.
Cloud application security awareness	Controls enterprise cloud applications in a refined and differentiated manner to meet enterprises' requirements for cloud application management.
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 user-defined signatures. Supports brute-force cracking detection based on user behaviors, and user-defined statistical periods.
Anti-Botnet	Support detects the Botnet traffic by use the intrusion prevention protection function.
Antivirus	Supports intelligent antivirus engine that can detect hundreds of millions of virus variants.
Anti-Spyware	Support uses antivirus engine to detect Spyware software.
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 140 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. Supports the SafeSearch function to filter resources of search engines, such as Google, to guarantee access to only healthy network resources.
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.

Feature	Description
Anti-DDoS	Defends against more than 10 types of common DDoS attacks, including SYN flood and UDP flood attacks.
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.
Deployment and reliability	Supports transparent, routing, and hybrid working modes and high availability (HA), including the Active/Active and Active/Standby modes.

Specifications

System Performance and Capacity

Model	USG6615F	USG6625F	USG6635F	USG6655F
Firewall Throughput[1] (1518/512/64-byte, UDP)	15/15/15 Gbit/s	25/25/25 Gbit/s	35/35/35 Gbit/s	50/50/40 Gbit/s
Firewall Latency (64-byte, UDP)	18 μs	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]	8 Gbps	12 Gbps	18 Gbps	25 Gbps
NGFW Throughput[3]	6 Gbps	10 Gbps	12 Gbps	18 Gbps
NGFW Throughput (Enterprise Mix)[4]	4.6 Gbps	4.6 Gbps	8 Gbps	8 Gbps
Threat Protection Throughput (Enterprise Mix)[5]	4 Gbps	4 Gbps	7 Gbps	7 Gbps
IPsec VPN Throughput[1] (AES-256 + SHA256, 1420-byte)	15 Gbit/s	25 Gbit/s	30 Gbit/s	30 Gbit/s
SSL VPN Throughput[6]	1 Gbit/s	1.5 Gbit/s	3 Gbit/s	3 Gbit/s
Concurrent SSL VPN Users * (Default/Maximum)	2000	2000	5000	5000
Security Policies (Maximum)	40,000	40,000	60,000	60,000
Virtual Firewalls	1000	1000	1000	1000

Model	USG6615F	USG6625F	USG6635F	USG6655F
URL Filtering: Categories	More than 130			
URL Filtering: URLs	A database of over 120 million URLs in the cloud			
Automated Threat Feedback and 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-part management software based on SNMP, SSH, and Syslog			
VLANs (Maximum)	4094			
VLANIF Interfaces (Maximum)	4094			

Model	USG6685F	USG6710F	USG6715F	USG6725F
Firewall Throughput[1] (1518/512/64-byte, UDP)	80/80/40 Gbit/s	100/100/60 Gbit/s	160/160/80 Gbit/s	240/240/120 Gbit/s
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]	25 Gbps	45 Gbps	50 Gbps	75 Gbps
NGFW Throughput[3]	18 Gbps	30 Gbps	36 Gbps	54 Gbps
NGFW Throughput (Enterprise Mix)[4]	8 Gbps	16 Gbps	16 Gbps	24 Gbps
Threat Protection Throughput (Enterprise Mix)[5]	7 Gbps	14 Gbps	14 Gbps	21 Gbps
IPsec VPN Throughput[1] (AES-256 + SHA256, 1420-byte)	30 Gbit/s	40 Gbit/s	45 Gbit/s	65 Git/s
SSL VPN Throughput [6]	5 Gbit/s	10 Gbit/s	10 Gbit/s	12 Gbit/s
Concurrent SSL VPN Users * (Default/Maximum)	100/5000	100/10000	100/10000	100/15000
Security Policies (Maximum)	60,000	60,000	60,000	60,000
Virtual Firewalls	1000	1000	1000	1000
URL Filtering: Categories	More than 130			
URL Filtering: URLs	A database of over 120 million URLs in the cloud			
Automated Threat Feedback and 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-part management software based on SNMP, SSH, and Syslog			

Model	USG6685F	USG6710F	USG6715F	USG6725F
VLANs (Maximum)	4094			
VLANIF Interfaces (Maximum)	1024			

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.

*SA: indicates service awareness.

Hardware Specifications

Model	USG6615F	USG6625F	USG6635F	USG6655F
Dimensions (H×W×D) mm	43.6×442×420			
Form Factor/Height	1U			
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×USB 3.0			
Weight	6.3 kg		7.3 kg	
External Storage	Optional, SATA (1×2.5 inch) supported, 240 GB/ 1TB			
Power Supply	100 V to 240 V			
Maximum power consumption of the machine	222W		242W	
Power Supplies	Optional dual AC 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			

Model	USG6685F	USG6710F	USG6715F	USG6725F
Dimensions (H×W×D) mm	43.6×442×420			
Form Factor/Height	1U			
Fixed Interface	8×GE COMBO + 4×GE(RJ45)+ 10×10GE(SFP+)	2×100GE(QSFP28) + 2×40G(QSFP+) + 8×25(ZSFP+) + 20×10GE(SFP+)[1]		4×100GE(QSFP28) + 16×25GE(ZSFP+) + 8×10GE(SFP+)[2]

Model	USG6685F	USG6710F	USG6715F	USG6725F
USB Port	1×USB 3.0			
Weight	7.3 kg		10.2 kg	
External Storage	Optional, SATA (1×2.5 inch) supported, 240 GB/ 1TB			
Power Supply	100 V to 240 V			
Maximum power consumption of the machine	222W		242W	
Power Supplies	Optional dual AC 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.

Ordering Information

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)
USG6625F	USG6625F-AC	USG6625F AC Host (8*GE COMBO + 4*GE RJ45 + 4*GE SFP + 6*10GE SFP+, 1 AC power supply)
USG6635F	USG6635F-AC	USG6635F AC Host (8*GE COMBO + 4*GE RJ45 + 10*10GE SFP+, 2 AC power supplies)
USG6655F	USG6655F-AC	USG6655F AC Host (8*GE COMBO + 4*GE RJ45 + 10*10GE SFP+, 2 AC power supplies)
USG6685F	USG6685F-AC	USG6685F AC Host (8*GE COMBO + 4*GE RJ45 + 10*10GE SFP+, 2 AC power supplies)
USG6710F	USG6710F-AC	USG6710F AC Host (2*QSFP28 + 2*QSFP+ + 8*ZSFP+ + 20*SFP+, 2 AC power supplies)
USG6715F	USG6715F-AC	USG6715F AC Host (2*QSFP28 + 2*QSFP+ + 8*ZSFP+ + 20*SFP+, 2 AC power supplies)
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)
	LIC-USG6KF-VSYS-50	Quantity of Virtual Firewall (50 Vsys)
	LIC-USG6KF-VSYS-100	Quantity of Virtual Firewall (100 Vsys)

Product	Model	Description
	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 12 Months (Applies to USG6615F)
	LIC-USG6625F-IPS-1Y	IPS Update Service Subscribe 12 Months (Applies to USG6625F)
	LIC-USG6635F-IPS-1Y	IPS Update Service Subscribe 12 Months (Applies to USG6635F)
	LIC-USG6655F-IPS-1Y	IPS Update Service Subscribe 12 Months (Applies to USG6655F)
	LIC-USG6685F-IPS-1Y	IPS Update Service Subscribe 12 Months (Applies to USG6685F)
	LIC-USG6710F-IPS-1Y	IPS Update Service Subscribe 12 Months (Applies to USG6710F)
	LIC-USG6715F-IPS-1Y	IPS Update Service Subscribe 12 Months (Applies to USG6715F)
	LIC-USG6725F-IPS-1Y	IPS Update Service Subscribe 12 Months (Applies to USG6725F)
URL Filtering Update Service	LIC-USG6615F-URL-1Y	URL Update Service Subscribe 12 Months (Applies to USG6615F)
	LIC-USG6625F-URL-1Y	URL Update Service Subscribe 12 Months (Applies to USG6625F)
	LIC-USG6635F-URL-1Y	URL Update Service Subscribe 12 Months (Applies to USG6635F)
	LIC-USG6655F-URL-1Y	URL Update Service Subscribe 12 Months (Applies to USG6655F)
	LIC-USG6685F-URL-1Y	URL Update Service Subscribe 12 Months (Applies to USG6685F)
	LIC-USG6710F-URL-1Y	URL Update Service Subscribe 12 Months (Applies to USG66710F)
	LIC-USG6715F-URL-1Y	URL Update Service Subscribe 12 Months (Applies to USG6715F)
	LIC-USG6725F-URL-1Y	URL Update Service Subscribe 12 Months (Applies to USG6725F)

Product	Model	Description
Antivirus Update Service	LIC-USG6615F-AV-1Y	AV Update Service Subscribe 12 Months (Applies to USG6615F)
	LIC-USG6625F-AV-1Y	AV Update Service Subscribe 12 Months (Applies to USG6625F)
	LIC-USG6635F-AV-1Y	AV Update Service Subscribe 12 Months (Applies to USG6635F)
	LIC-USG6655F-AV-1Y	AV Update Service Subscribe 12 Months (Applies to USG6655F)
	LIC-USG6685F-AV-1Y	AV Update Service Subscribe 12 Months (Applies to USG6685F)
	LIC-USG6710F-AV-1Y	AV Update Service Subscribe 12 Months (Applies to USG6710F)
	LIC-USG6715F-AV-1Y	AV Update Service Subscribe 12 Months (Applies to USG6715F)
	LIC-USG6725F-AV-1Y	AV Update Service Subscribe 12 Months (Applies to USG6725F)
Threat Protection Bundle (IPS, AV, URL)	LIC-USG6615F-TP -1Y-OVS	Threat Protection Subscription 12 Months (Applies to USG6615F Overseas)
	LIC-USG6625F-TP-1Y-OVS	Threat Protection Subscription 12 Months (Applies to USG6625F Overseas)
	LIC-USG6635F-TP-1Y-OVS	Threat Protection Subscription 12 Months (Applies to USG6635F Overseas)
	LIC-USG6655F-TP-1Y-OVS	Threat Protection Subscription 36 Months (Applies to USG6655F Overseas)
	LIC-USG6685F-TP -1Y-OVS	Threat Protection Subscription 12 Months (Applies to USG6685F Overseas)
	LIC-USG6710F-TP-1Y-OVS	Threat Protection Subscription 12 Months (Applies to USG6710F Overseas)
	LIC-USG6715F-TP-1Y-OVS	Threat Protection Subscription 12 Months (Applies to USG6715F Overseas)
	LIC-USG6725F-TP-1Y-OVS	Threat Protection Subscription 36 Months (Applies to USG6725F Overseas)
N1 License		
N1	N1-USG6685F-A-Lic	N1-USG6685F Advanced, Per Device
	N1-USG6685F-A-SnS1Y	N1-USG6685F Advanced, SnS, Per Device, 1 Year
	N1-USG6685F-F-Lic	N1-USG6685F Foundation, Per Device
	N1-USG6685F-F-SnS1Y	N1-USG6685F Foundation, SnS, Per Device, 1 Year
	N1-USG6710F-A-Lic	N1-USG6710F Advanced, Per Device
	N1-USG6710F-A-SnS1Y	N1-USG6710F Advanced, SnS, Per Device, 1 Year

Product	Model	Description
	N1-USG6710F-F-Lic	N1-USG6710F Foundation, Per Device
	N1-USG6710F-F-SnS1Y	N1-USG6710F Foundation, SnS, Per Device, 1 Year
	N1-USG6715F-A-Lic	N1-USG6715F Advanced, Per Device
	N1-USG6715F-A-SnS1Y	N1-USG6715F Advanced, SnS, Per Device, 1 Year
	N1-USG6715F-F-Lic	N1-USG6715F Foundation, Per Device
	N1-USG6715F-F-SnS1Y	N1-USG6715F Foundation, SnS, Per Device, 1 Year
	N1-USG6725F-A-Lic	N1-USG6725F Advanced, Per Device
	N1-USG6725F-A-SnS1Y	N1-USG6725F Advanced, SnS, Per Device, 1 Year
	N1-USG6725F-F-Lic	N1-USG6725F Foundation, Per Device
	N1-USG6725F-F-SnS1Y	N1-USG6725F Foundation, SnS, Per Device, 1 Year
	N1-USG6615F-F-Lic	N1-USG6615F Foundation, Per Device
	N1-USG6615F-F-SnS1Y	N1-USG6615F Foundation, SnS, Per Device, 1 Year
	N1-USG6615F-A-Lic	N1-USG6615F Advanced, Per Device
	N1-USG6615F-A-SnS1Y	N1-USG6615F Advanced, SnS, Per Device, 1 Year
	N1-USG6625F-F-Lic	N1-USG6625F Foundation, Per Device
	N1-USG6625F-F-SnS1Y	N1-USG6625F Foundation, SnS, Per Device, 1 Year
	N1-USG6625F-A-Lic	N1-USG6625F Advanced, Per Device
	N1-USG6625F-A-SnS1Y	N1-USG6625F Advanced, SnS, Per Device, 1 Year
	N1-USG6635F-F-Lic	N1-USG6635F Foundation, Per Device
	N1-USG6635F-F-SnS1Y	N1-USG6635F Foundation, SnS, Per Device, 1 Year
	N1-USG6635F-A-Lic	N1-USG6635F Advanced, Per Device
	N1-USG6635F-A-SnS1Y	N1-USG6635F Advanced, SnS, Per Device, 1 Year
	N1-USG6655F-F-Lic	N1-USG6655F Foundation, Per Device
	N1-USG6655F-F-SnS1Y	N1-USG6655F Foundation, SnS, Per Device, 1 Year
	N1-USG6655F-A-Lic	N1-USG6655F Advanced, Per Device
	N1-USG6655F-A-SnS1Y	N1-USG6655F Advanced, SnS, 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.