HUAWEI USG6600 Next-Generation Firewall

With the proliferation of smart devices, such as smartphones and tablets, mobile apps, Web2.0, and social networking become integral parts of enterprise operation. The wide use of mobile devices improves the communication efficiency for enterprises, but blurs network borders and complicates security issues. Moreover, the traditional firewalls that implement access control only by IP address and port cannot cope with ever-increasing application layer threats.

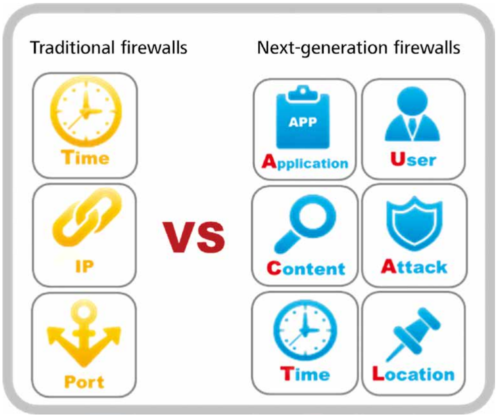
Against this background, Huawei launches the USG6600 series next-generation firewall to address these issues. The USG6600 is designed for large- and medium-sized enterprises and next-generation data centers. The USG6600 provides fine-grained service access control and service acceleration through context awareness by Application, Content, Time, User, Attack, or location (ACTUAL). The USG6600 integrates application-layer protection functions, such as Intrusion Prevention System (IPS) and antivirus with application identification technologies to improve the threat defense efficiency and accuracy. The USG6600 is a multi-purpose device that provides comprehensive protection to reduce the management cost. Fine-grained bandwidth management and QoS optimization greatly reduce enterprises' bandwidth leasing fees and ensure user experience in mission-critical services. In short, the USG6600 is a simple and efficient device that provides up-to-date next-generation security.

Product Appearance

USG6600 next-generation firewalls

Product Features and Benefits

Accurate Access Control



Compared with traditional firewalls, the USG6600 provides fined-grained and more accurate access control. The USG6600 has the following features:

- **Integrated protection:** The USG6600 implements access control and protection by Application, Content, Time, User, Attack, or location (ACTUAL). It integrates application-layer defense and application identification. For example, the USG6600 can identify Oracle traffic and implement intrusion prevention specially for Oracle traffic to increase efficiency and reduce false positive rate.
- **Application-specific:** The USG6600 accurately identifies over 6000 applications (including mobile and web applications) and their functions, and then implements access control and service acceleration. For example, the USG6600 can identify the voice and data services of an instant message and apply different control policies for the services.
- **User-specific:** The USG6600 supports eight user authentication methods, such as RADIUS, LDAP, and AD authentication and synchronizes user information from the existing user authentication system. The USG6600 implements access control, QoS management, and in-depth protection by user.
- **Location-specific:** Based on the mappings between IP addresses and geographical locations, the USG6600 identifies the locations from which application traffic and attack traffic originates and promptly detects network exceptions. Then the USG6600 implements differentiated access control for locations, which can be user-defined for IP addresses.

Overall Protection

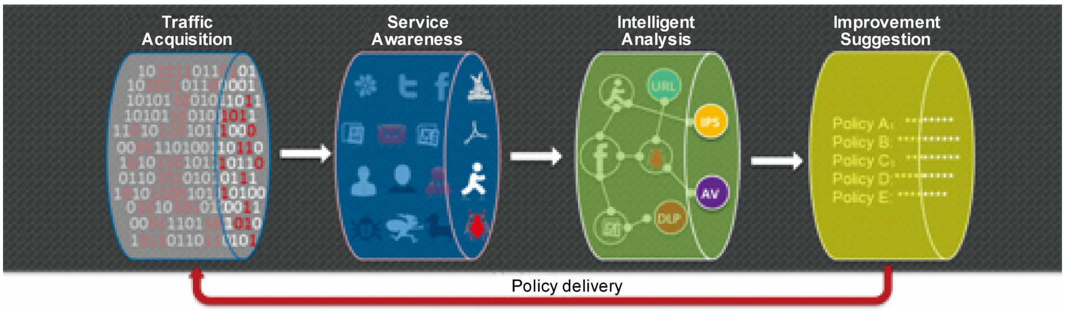
As more information assets are accessible from the Internet, network attacks and information have been industrialized, requiring wider ranges of protections form next-generation firewalls. The USG6600 provides overall protection:

- **Multi-purpose:** The USG6600 integrates the traditional firewall, VPN, intrusion prevention, antivirus, data leak prevention, bandwidth management, and online behavior management functions all in one device, simplifying device deployment and improving management efficiency.
- **IPS:** The USG6600 can detect and defend against over 5000 vulnerabilities. It can identify and defend against web application attacks, such as cross-site scripting and SQL injection attacks.
- **Antivirus:** The high-performance antivirus engine of the USG6600 can defend against over five million viruses and Trojan horse. The virus signature database is updated daily.

- **APT Defense:** Firewall can interwork with the Sandbox to realize the unknown threat prevention. The firewall can identify and extract the doubtful traffic in the type of file from network traffic, and send it to the Sandbox for threat analysis. The Sandbox can check whether the traffic is malicious by analyzing and identifying the behaviors of the unknown file after the file is run. The firewall then processes the traffic according to the detection results given by the Sandbox.
- **Data leak prevention:** The USG6600 identifies and filters the files and content to be transferred. It can identify more than 120 file types to prevent virus attacks that are launched by modifying file name extensions. It can restore and implement content filtering for over 30 types of files, such as word, excel, PPT, PDF, and RAR files to prevent leaks of critical enterprise information.
- **SSL decryption:** The USG6600 serves as a proxy and implements application-layer protection for SSL-encrypted traffic, such as IPS, AV, data leak prevention, and URL filtering.
- **Anti-DDoS:** The USG6600 can identify and defend against over 5 million viruses and over 10 types of DDoS attacks, such as SYN flood and UDP flood attacks.
- **Online behavior management:** The USG6600 implements cloud-based URL category filtering to prevent threats caused by users' access to malicious websites and control users' online behaviors, such as posting. The USG6600 has a predefined URL category database that contains over 85 million URLs. In addition, the USG6600 audits users' network access records, such as posting and FTP operations.
- **Secure interconnection:** The USG6600 supports various VPN features, such as IPSec, SSL, L2TP, MPLS, and GRE VPN to ensure high-availability and secure interconnection between enterprise headquarters and branch offices.
- **CPU attack defense:** The USG6600 supports different upload rates for different protocol packets to avoid the impact of the CPU by a large number of protocol packets and to protect the CPU.
- **QoS management:** The USG6600 flexibly controls upper and lower traffic thresholds and implements policy-based routing and QoS marking by application. It supports QoS marking for URL categories. For example, the packets for accessing financial websites are assigned a higher priority.
- **Load balancing:** The USG6600 supports server load balancing. In a multi-egress scenario, the USG6600 can implement load balancing with the egresses for applications according to link quality, bandwidth, and weights.
- **Virtualization:** The USG6600 supports virtualization of multiple security services, such as firewall, intrusion prevention, antivirus, and VPN services and implements independent management for different users on the same physical device.
- Prevent Advanced Persistent Threat (APT) attacks using a reputation system.

Simple Security Management

- **SmartPolicy**



Next-generation firewalls provide a wider range of protections and more accurate access control than traditional firewalls. As a result, the configuration of the next-generation firewalls is complex, imposing higher requirements on the experience and skills of administrators. To reduce administration complexity, the USG6600 provides the smart policy feature, which has the following functions:

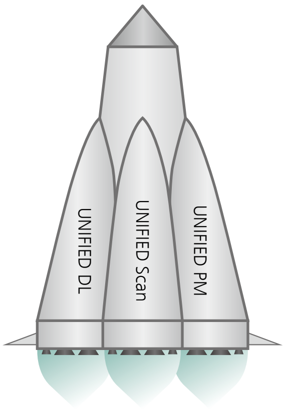
- **Rapid deployment policy:** The built-in scenario policy template allows administrators to rapidly deploy common protection policies without heavily relying on their experience and skills. For example, to use the network storage, the administrator can use only the "network disk" policy template to set up a series of policies. The policies allow users to download applications of the network disk category and perform virus detection but prevents them from uploading files.
- **Intelligent optimization policy:** The USG6600 generates policy tuning suggestions based on network traffic and application risks in compliance with the minimum privilege principle. The function is helpful when an enterprise needs to transform a large number of port-based firewall policies to application-based next-generation firewall policies.
- **Intelligent policy cleanup:** The USG6600 automatically discovers redundant and inactive policies for policy cleanup.

• Network Security Report

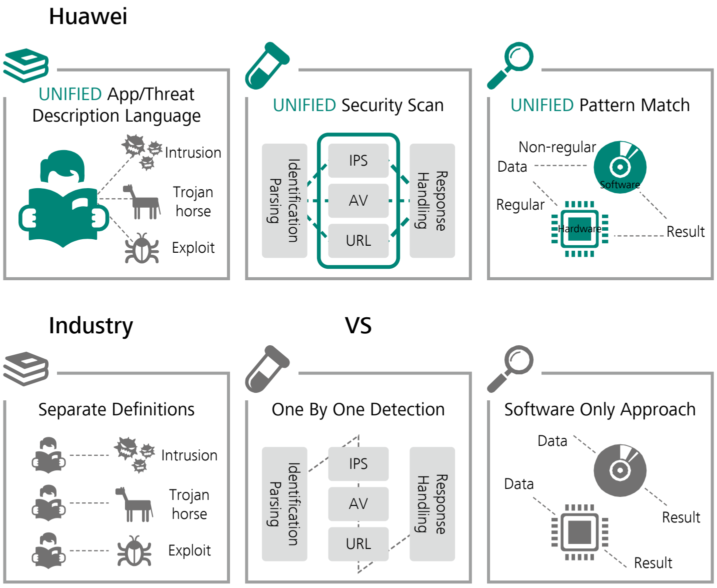
Enterprise administrators can perform assessment over the current network security status by the network security report and providing the related optimization suggestions. An administrator can export the original report data from the Firewall and upload the original data file to Huawei security center (sec.huawei.com). Then a network security report is generated for the administrator. This report provides diversified reports (in pie charts, bar charts, and curve charts). These reports display traffic, threat, web page browsing, and data leak analysis results, from which the administrator can gain visibility into network security.

High Protection Performance

The performance of the UTM that has the application-layer protection function enabled is deteriorated and cannot meet current application-layer protection requirements. In contrast, the next-generation firewalls can retain high-performance when providing multiple-level protection.



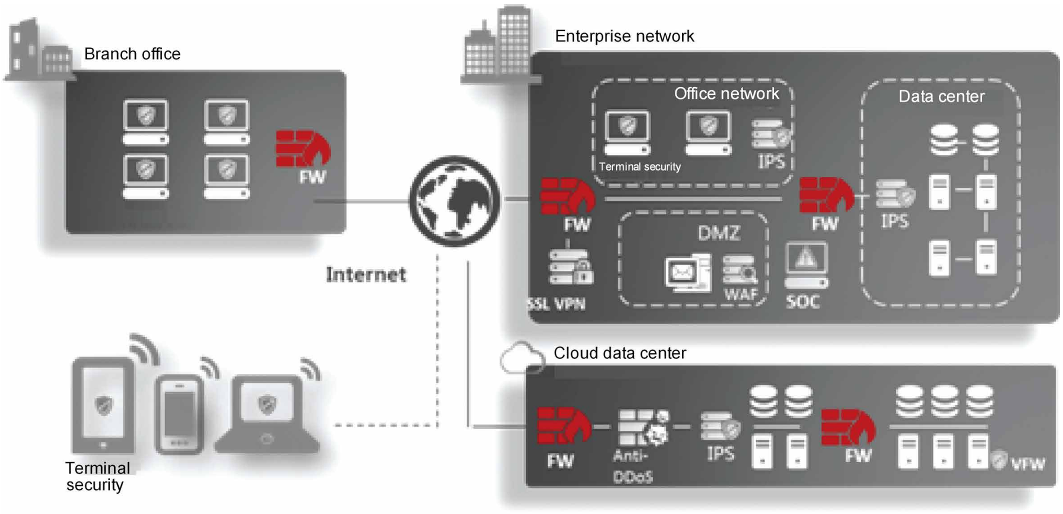
Everything UNIFIED for High Performance



The USG6600 uses the intelligence awareness engine (IAE) to ensure high performance in case of multiple-level protection. The IAE uses three core technologies:

- **Unified signature description language:** Application, IPS, and antivirus signatures are described in a unified language so that the USG6600 can match traffic with these signatures concurrently to improve the traffic processing efficiency.
- **Integrated architecture:** Unlike the serial processing of UTM security functions, the security services of the USG6600 are parallel. Therefore, the USG6600 can have multiple security services enabled and still retain high performance.
- **Hardware acceleration:** The USG6600 uses dedicated hardware for resource-consuming computing, such as packet encryption and decryption and regular expression matching. For common services, the USG6600 still uses the CPU for computing.

Typical Application Scenarios



Intranet Border Protection

- Deploy next-generation firewalls on intranet borders to control access by user.
- Implement user- and application-based policy control on mobile users for refined permission management and logging.
- Implement content filtering and auditing on email transfer, IM, and file transfer to monitor social networking applications and prevent data leaks.

Internet Egress Protection

- Deploy a next-generation firewall at the Internet egress to implement access control and prevent unauthorized access.
- Enable intrusion prevention and provide 10-Gigabit level application-layer protection.
- Implement content filtering and auditing on email transfer, IM, and file transfer to monitor social networking applications and prevent data leaks.
- Implement user-, application-, and time-based QoS management to preferentially guarantee the service qualities for mission-critical users and services.

- Use URL categories and application blocking to prevent Trojan horse websites and non-work-related websites and monitor the accessible websites and network applications.

Cloud Data Center Border Protection

- Deploy a next-generation firewall which virtualizes all security services and system resources to provide exceptional experience for each virtual system.
- Enable the 10-Gigabit level intrusion prevention function to effectively block attacks and provide differentiated defense functions in different virtual systems.
- Enable anti-DDoS to remove DDoS traffic and protect data centers.

Remote VPN Access

- Deploy a next-generation firewall to establish reliable, controllable, and manageable tunnels for secure data transfer on the Internet.
- Provide SSL VPN across multiple platforms (including Windows, IOS, Android, Blackberry, and Symbian).

Specifications

Model	USG6620	USG6630	USG6650	USG6660	USG6670	USG6680
Firewall throughput* (1518bytes)	12 Gbit/s	16 Gbit/s	20 Gbit/s	25 Gbit/s	35 Gbit/s	40 Gbit/s
IPS throughput	5.8Gbit/s	5.8Gbit/s	8.8Gbit/s	8.8Gbit/s	8.8Gbit/s	15Gbit/s
IPS+AV throughput	5Gbit/s	5Gbit/s	8Gbit/s	8Gbit/s	8Gbit/s	13Gbit/s
Concurrent sessions	6,000,000	6,000,000	8,000,000	10,000,000	10,000,000	12,000,000
New sessions per second	200,000	250,000	300,000	350,000	400,000	400,000
VPN Throughput* (IPSec, AES, 1420 byte)	12 Gbit/s	12 Gbit/s	15 Gbit/s	18 Gbit/s	18Gbit/s	18 Gbit/s
Virtual firewalls	200	200	500	500	500	1,000
MTBF	10.08years	10.08years	27.07years	27.07years	23.67years	19.18years
MTTR	5.95min	5.95min	2.22min	2.22min	2.53min	3.13min

Model	USG6620	USG6630	USG6650	USG6660	USG6670	USG6680
Maximum power	170W		350 W	350 W		700W
DC power supply	-		-	-48 V to -60 V		
AC power supply	100 V to 240 V		100 V to 240 V			
Fixed port	8GE+4SFP		2 x 10GE+8GE+8SFP		4 x 10GE+16GE+8SFP	
Expansion Slots	2 x WSIC		6 x WSIC		5 x WSIC	
Interface module	WSIC: 2 x 10GE (SFP+)+8 x GE (RJ45), 8 x GE (RJ45), 8 x GE (SFP), 4 x GE (RJ45) BYPASS					
Height	1U		3U			
Dimensions (W×D×H)	442mm×421mm×44.4mm		442mm×470mm×130.5mm			
Weight (full configuration)	10 kg		24 kg			
HDD	Optional. Supports single 300 GB hard disks (hot swappable).		Optional. Supports 300 GB hard disks (RAID1 and hot swappable).			
Redundant power supply	Optional		Standard configuration			
Operating environment	Temperature: 0°C to 40°C/5°C to 40°C(with optional HDD) Humidity: 10% to 90%					
Non-operating environment	Temperature: -40°C to 70°C Humidity: 5% to 95%					

* The throughput is based on 1518 or 1420 byte packet size and tested under ideal conditions. Real result may vary with different deployment environments.

Certifications	
Software	ICSA Labs: Firewall, IPS, IPSec, SSL VPN CC: EAL4+ NSS Labs: Recommended Rating
Hardware	CB, CCC, CE-SDOC, ROHS, REACH&WEEE(EU), C-TICK, ETL, FCC&IC, VCCI, BSMI

Functions

Functions	
Context awareness	ACTUAL (Application, Content, Time, User, Attack, Location)–based awareness capabilities
	Eight authentication methods (local, RADIUS, HWTACACS, SecureID, AD, CA, LDAP, and Endpoint Security)
Application security	Fine-grained identification of over 6000 application protocols, application-specific action, and online update of protocol databases
	Combination of application identification and virus scanning to recognize the viruses (more than 5 millions), Trojan horses, and malware hidden in applications
	Combination of application identification and content detection to identify file types and sensitive information to prevent information leaks
Intrusion prevention	Provides over 5000 signatures for attack identification.
	Provides protocol identification to defend against abnormal protocol behaviors.
	Supports user-defined IPS signatures.
	Supports APT defense. Interworking with the Sandbox to detect and block the malicious files in the network.
Web security	Cloud-based URL filtering with a URL category database that contains over 130 million URLs in over 80 categories
	Defense against web application attacks, such as cross-site scripting and SQL injection attacks
	HTTP/HTTPS/FTP-based content awareness to defend against web viruses
	URL blacklist and whitelist and keyword filtering
Email security	Real-time anti-spam to detect and filter out phishing emails
	Local whitelist and blacklist, remote real-time blacklist, content filtering, keyword filtering, and mail filtering by attachment type, size, and quantity
	Virus scanning and notification for POP3/SMTP/IMAP email attachments

Functions	
Data security	Data leak prevention based on content awareness
	File reassembly and data filtering for more than 30 file types (including Word, Excel, PPT, and PDF), and file blocking for more than 120 file types
Security virtualization	Virtualization of security features, forwarding statistics, users, management operations, views, and resources (such as bandwidths and sessions)
Network security	Defense against more than 10 types of DDoS attacks, such as the SYN flood and UDP flood attacks
	VPN technologies: IPSec VPN, SSL VPN, L2TP VPN, MPLS VPN, and GRE
Routing	IPv4: static routing, RIP, OSPF, BGP, and IS-IS IPv6: RIPng, OSPFv3, BGP4+, IPv6 IS-IS, IPv6 RD, and ACL6
Working mode and availability	Transparent, routing, or hybrid working mode and high availability (HA), including the Active/Active and Active/Standby mode
Intelligent management	Evaluates the network risks based on the passed traffic and intelligently generates policies based on the evaluation to automatically optimize security policies. Supports policy matching ratio analysis and the detection of conflict and redundant policies to remove them, simplifying policy management.
	Provides a global configuration view and integrated policy management. The configurations can be completed in one page.
	Provides visualized and multi-dimensional report display by user, application, content, time, traffic, threat, and URL.
	Enterprise administrators can perform assessment over the current network security status by the network security report and providing the related optimization suggestions.

Ordering Guide

Model	Description
Main Equipment	
USG6620-AC	USG6620 AC Host(8GE(RJ45)+4GE(SFP), 8GB Memory, 1 AC Power), with HW General Security Platform Software
USG6620-BDL-AC	USG6620 AC Host(8GE(RJ45)+4GE(SFP), 8GB Memory, 1 AC Power, with IPS-AV-URL Function Group Update Service Subscribe 12 Months), with HW General Security Platform Software

Model	Description
USG6630-AC	USG6630 AC Host(8GE(RJ45)+4GE(SFP), 8GB Memory, 1 AC Power), with HW General Security Platform Software
USG6630-BDL-AC	USG6630 AC Host(8GE(RJ45)+4GE(SFP), 8GB Memory, 1 AC Power, with IPS-AV-URL Function Group Update Service Subscribe 12 Months), with HW General Security Platform Software
USG6650-AC	USG6650 AC Host(8GE(RJ45)+8GE (SFP)+2*10GE(SFP+), 16G Memory, 2 AC Power), with HW General Security Platform Software
USG6650-BDL-AC	USG6650 AC Host(8GE(RJ45)+8GE (SFP)+2*10GE(SFP+), 16G Memory, 2 AC Power, with IPS-AV-URL Function Group Update Service Subscribe 12 Months), with HW General Security Platform Software
USG6660-AC	USG6660 AC Host(8GE(RJ45)+8GE(SFP)+2*10GE(SFP+), 16G Memory, 2 AC Power), with HW General Security Platform Software
USG6660-BDL-AC	USG6660 AC Host(8GE(RJ45)+8GE(SFP)+2*10GE(SFP+), 16G Memory, 2 AC Power, with IPS-AV-URL Function Group Update Service Subscribe 12 Months), with HW General Security Platform Software
USG6660-DC	USG6660 DC Host(8GE(RJ45)+8GE(SFP)+2*10GE(SFP+), 16G Memory, 2 DC Power), with HW General Security Platform Software
USG6670-AC	USG6670 AC Host(16GE(RJ45)+8GE(SFP)+4*10GE(SFP), 16G Memory, 2 AC Power), with HW General Security Platform Software
USG6670-BDL-AC	USG6670 AC Host(16GE(RJ45)+8GE(SFP)+4*10GE(SFP), 16G Memory, 2 AC Power, with IPS-AV-URL Function Group Update Service Subscribe 12 Months), with HW General Security Platform Software
USG6670-DC	USG6670 DC Host(16GE(RJ45)+8GE(SFP)+4*10GE(SFP), 16G Memory, 2 DC Power), with HW General Security Platform Software
USG6680-AC	USG6680 AC Host(16GE(RJ45)+8GE(SFP)+4*10GE(SFP+), 16G Memory, 2 AC Power), with HW General Security Platform Software
USG6680-BDL-AC	USG6680 AC Host(16GE(RJ45)+8GE(SFP)+4*10GE(SFP+), 16G Memory, 2 AC Power, with IPS-AV-URL Function Group Update Service Subscribe 12 Months), with HW General Security Platform Software
USG6680-DC	USG6680 DC Host(16GE(RJ45)+8GE(SFP)+4*10GE(SFP+), 16G Memory, 2 DC Power), with HW General Security Platform Software
Business Module Group	
WSIC-8GE	8GE Electric Ports Interface Card, with HW General Security Platform Software

Model	Description
WSIC-4GEBYPASS	4GE Electric Ports Bypass Card, with HW General Security Platform Software
WSIC-8GEF	8GE Optical Ports WSIC Interface Card, with HW General Security Platform Software
WSIC-2XG8GE	2*10GE Optical Ports+8GE Electric Ports Interface Card, with HW General Security Platform Software
Hard disk Group	
SM-HDD-SAS300G-A	300GB 10K RPM SAS Hard Disk Unit
SM-HDD-SAS300G-B	300GB 10K RPM SAS Hard Disk for 1U rack Gateway
Option Power Group	
Power-AC-B	The AC power extension module-25degC-60degC-90V-290V-12V/14.2A
Optical Transmitter Module Collection	
OSX040N01	Optical Transceiver, SFP+, 10G, Single-mode Module(1550nm, 40km, LC)
OSU015N00	Optical Transceiver, eSFP, 2.5G, Single-mode Module(1310nm, 15km, LC)
SFP-GE-LX-SM1310	Optical Transceiver, eSFP, GE, Single-mode Module(1310nm, 10km, LC)
eSFP-GE-SX-MM850	Optical Transceiver, eSFP, GE, Multi-mode Module(850nm, 0.5km, LC)
S-SFP-GE-LH40-SM1310	Optical Transceiver, eSFP, GE, Single-mode Module(1310nm, 40km, LC)
OMXD30000	Optical Transceiver, SFP+, 10G, Multi-mode Module(850nm, 0.3km, LC)
OSX010000	Optical Transceiver, SFP+, 10G, Single-mode Module(1310nm, 10km, LC)
OSX040N01	Optical Transceiver, SFP+, 10G, Single-mode Module(1550nm, 40km, LC)
OSU015N00	Optical Transceiver, eSFP, 2.5G, Single-mode Module(1310nm, 15km, LC)
SFP-GE-LX-SM1310	Optical Transceiver, eSFP, GE, Single-mode Module(1310nm, 10km, LC)
Installation Material	
SU5M1RAIL01	Cabinet Guide Rail
QW1P0FIBER06	Optical adapter-LC/PC-LC/PC-Blue-Shell: Plastic-Sleeve: Zirconia-Square
SS-OP-D-LC-M-5	Patch cord-LC/PC-LC/PC-Multimode-A1b-2mm-5m-PVC-Orange
SS-OP-D-LC-M-10	Patch cord-LC/PC-LC/PC-Multimode-A1b-2mm-10m-PVC-Orange

Model	Description
SS-OP-D-LC-M-20	Patch cord-LC/PC-LC/PC-Multimode-A1b-2mm-20m-PVC-Orange
SS-OP-D-LC-S-6	Patch cord-LC/PC-LC/PC-Single mode-G.652D-2mm-6m-PVC-Yellow
SS-OP-D-LC-S-10	Patch cord-LC/PC-LC/PC-Single mode-G.652D-2mm-10m-PVC-Yellow
SS-OP-D-LC-S-20	Patch cord-LC/PC-LC/PC-Single mode-G.652-2mm-20m-PVC-Yellow
SS-OP-LC-SC-M-20	Patch cord-LC/PC-SC/PC-Multimode-A1b-2mm-20m-PVC-Orange
SS-OP-LC-SC-S-20	Patch cord-LC/PC-SC/PC-Single mode-G.652-2mm-20m-PVC-Yellow
SS-OP-LC-FC-M-10	Patch cord-FC/PC-LC/PC-Multimode-A1b-2mm-10m-PVC-Orange
SS-OP-LC-FC-S-10	Patch cord-FC/PC-LC/PC-Single mode-G.652D-2mm-10m-PVC-Yellow
Function License	
LIC-VSYS-10-USG6000	Quantity of Virtual System(10 Vsys), with HW General Security Platform Software
LIC-VSYS-20-USG6000	Quantity of Virtual System(20 Vsys), with HW General Security Platform Software
LIC-VSYS-50-USG6000	Quantity of Virtual System(50 Vsys), with HW General Security Platform Software
LIC-VSYS-100-USG6000	Quantity of Virtual System(100 Vsys), with HW General Security Platform Software
LIC-VSYS-200-USG6000	Quantity of Virtual System(200 Vsys), with HW General Security Platform Software
LIC-VSYS-500-USG6000	Quantity of Virtual System(500 Vsys), with HW General Security Platform Software
LIC-VSYS-1000-USG6000	Quantity of Virtual System(1000 Vsys), with HW General Security Platform Software
LIC-SSL-100-USG6000	Quantity of SSL VPN Concurrent Users(100 Users), with HW General Security Platform Software
LIC-SSL-200-USG6000	Quantity of SSL VPN Concurrent Users(200 Users), with HW General Security Platform Software
LIC-SSL-500-USG6000	Quantity of SSL VPN Concurrent Users(500 Users), with HW General Security Platform Software
LIC-SSL-1000-USG6000	Quantity of SSL VPN Concurrent Users(1000 Users), with HW General Security Platform Software

Model	Description
LIC-SSL-2000-USG6000	Quantity of SSL VPN Concurrent Users(2000 Users), with HW General Security Platform Software
LIC-SSL-5000-USG6000	Quantity of SSL VPN Concurrent Users(5000 Users), with HW General Security Platform Software
NGFW License	
USG6600 License	
LIC-IPS-12-USG6600	IPS Update Service Subscribe 12 Months, With HW General Security Platform Software
LIC-IPS-36-USG6600	IPS Update Service Subscribe 36 Months, With HW General Security Platform Software
LIC-URL-12-USG6600	URL Filtering Update Service Subscribe 12 Months, With HW General Security Platform Software
LIC-URL-36-USG6600	URL Filtering Update Service Subscribe 36 Months, With HW General Security Platform Software
LIC-AV-12-USG6600	Anti-Virus Update Service Subscribe 12 Months, With HW General Security Platform Software
LIC-AV-36-USG6600	Anti-Virus Update Service Subscribe 36 Months, With HW General Security Platform Software
LIC-IPSAVURL-12-USG6600	IPS-AV-URL Function Group Subscribe 12 Months, With HW General Security Platform Software
LIC-IPSAVURL-36-USG6600	IPS-AV-URL Function Group Subscribe 36 Months, With HW General Security Platform Software
Basic License	
LIC-CONTENT	Content Filtering Function