

USG9500 Series

Terabit Level Next-Generation Firewall

The USG9500 is a new-generation, terabit-level, all-in-one DC firewall from Huawei for cloud service providers, large-scale DCs, and large-scale enterprise campus networks. The USG9500 provides terabit-level processing performance and 99.999% reliability. It integrates multiple security features such as Network Address Translation (NAT), Virtual Private Network (VPN), Intrusion Protection System (IPS), virtualization, and Service Awareness (SA) to help enterprises construct cloud computing-oriented DCs under border security protection and reduce the equipment room investment and Total Cost of Ownership (TCO) per Mbit/s.

Highlights

Most accurate access control – *ACTUAL-based comprehensive protection*

The core function of both traditional firewalls and NGFWs is access control. However, access control is based on port and IP address on traditional firewalls. In contrast, the USG9500 provides a more fine-grained access control:

- **Comprehensive protection:** Provides integrated control and protection based on application, content, time, user, attack, and location (ACTUAL). The application-layer protection and application identification are combined. For example, the USG9500 can identify Oracle-specific traffic and implement intrusion prevention accordingly to increase efficiency and reduce false positives.
- **Based on application:** Accurately identifies over 6000 applications (including mobile and web applications) and their services, and then implements access control and service acceleration accordingly. For example, the USG9500 can identify the voice and data services of an instant messaging application and apply different control policies to the services.
- **Based on user:** Supports eight user authentication methods, including RADIUS, LDAP, and AD authentication, synchronization of user information from an existing user authentication system, user-based access control, and QoS management.
- **Based on location:** Uses IP address geolocation to identify from where application and attack traffic originates, promptly detects network anomalies, and implements differentiated user-defined access control for traffic from different locations.



Most pragmatic NGFW features – equivalent to multiple devices to reduce TCO

As more information assets are accessible from the Internet, cyber-attacks and information theft are rampant, requiring a wider range of protection from next-generation firewalls. The USG9500 provides comprehensive protection:

- **Versatility:** Integrates traditional firewall functions, VPN, intrusion prevention, antivirus, data leak prevention (DLP), bandwidth management, and online behavior management into one device to simplify deployment and improve efficiency.
- **Intrusion prevention system (IPS):** Detects and prevents exploits of over 12000 vulnerabilities and web application attacks, such as cross-site scripting and SQL injection.
- **Antivirus (AV):** Prevents over 5 million viruses and Trojan horses using the high-performance antivirus engine and the daily-updated virus signature database.
- **Data leak prevention:** Identifies and filters file and content transfers. The USG9500 can identify more than 120 file types, regardless of whether file name extensions are maliciously changed. In addition, the USG9500 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:** Serves as a proxy to perform application-layer protection, such as IPS, AV, DLP, and URL filtering, for SSL-encrypted traffic.
- **Anti-DDoS:** Identifies and prevents 10 types of DDoS attacks, such as SYN and UDP flood attacks.
- **Online behavior management:** Implements cloud-based URL filtering to prevent threats from malicious websites by using a URL category database that contains 120 million URLs, controls online behaviors such as posting to social media and FTP upload and download, and audits Internet access records.
- **Secure interconnection:** Supports various VPN features, such as IPSec, L2TP, MPLS, and GRE VPN, to ensure secure and reliable connections between enterprise headquarters and branch offices.
- **QoS management:** Flexibly manages the upper and lower traffic thresholds and supports application-specific policy-based routing and QoS marking to preferentially forward traffic of specified URL categories, such as financial websites.
- **Load balancing:** Supports server load balancing, such as load balancing based on link quality, bandwidth, and weight in scenarios where multi-egresses are available.

Most advanced network processor + multi-core CPU + distributed architecture – allowing linear increase of performance to break the performance bottleneck

The USG9500 uses a hardware platform that is often used in core routers to provide modularized components. Each LPU has two network processors (NPs) to provide line rate forwarding. The SPU uses multi-core CPUs and a multi-threaded architecture, and each CPU has an application acceleration engine. These hardware advantages, combined with Huawei's optimized concurrent processing technology, increase CPU capacity to ensure the high speed parallel processing of multiple services, such as NAT and VPN. LPUs and SPUs function separately. The overall performance increases linearly with the number of SPUs so that customers can easily scale up the performance at a low cost.

With the revolutionary system architecture, the USG9500 is the industry's highest-performance security gateway in terms of throughput and concurrent connections. The dedicated traffic distribution technology allows for linear performance growth with the number of SPUs. The USG9500 delivers a maximum of 1.92 Tbps large-packet throughput, 2.56 billion concurrent connections, and 4095 virtual firewalls to meet the performance demand of high-end customers, such as television and broadcast companies, government agencies, energy companies, and education organizations.

Most stable and reliable security gateway – full redundancy to ensure service continuity

Network security is important for the normal operation of enterprises. To ensure the service continuity on high-speed networks, the USG9500 supports active/standby and active/active redundancy, port aggregation, VPN redundancy, and SPU load balancing. The USG9500 also supports dual-MPU active/

standby switchover, which is normally seen in high-end routers, to provide high availability. The mean time between failures (MTBF) of the USG9500 is up to 200,000 hours, and the failover time is less than one second.

Most diverse virtualization functions – *for cloud networks*

Cloud computing relies on virtualization and secure high-speed network connections. To support cloud technologies, the USG9500 delivers high throughput and supports virtual systems that have dedicated resources, independently forward traffic, and are configured and managed separately to meet the requirements of different customers. You can assign different resources to virtual systems as needed, configure different policies, log management, and audit functions on virtual systems based on the requirements of tenants, and customize traffic forwarding processes on virtual systems. The forwarding planes of virtual systems are separated to ensure the data security of tenants and that any resource exhaustion on one virtual system does not affect other virtual systems.

Solution Deployment Scenario

Background and Challenges

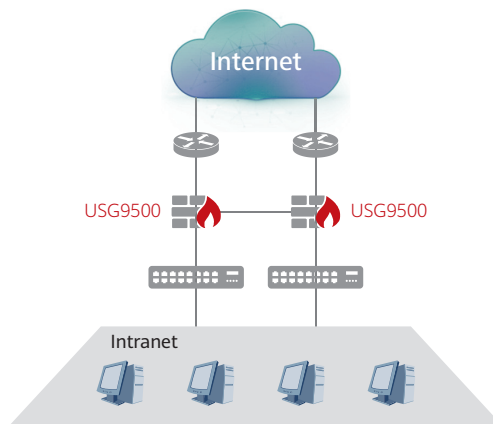
With the dramatic increase in the volume of enterprise data, data centers provide more types of services, handle more traffic, and become more important for enterprises—they also attract more hackers. Data centers have evolved from data concentration to server consolidation based on virtualization technologies in the cloud era. This evolution has brought security challenges to data centers. Now, security is the key factor that determines their efficiency and availability.

Customer Requirements

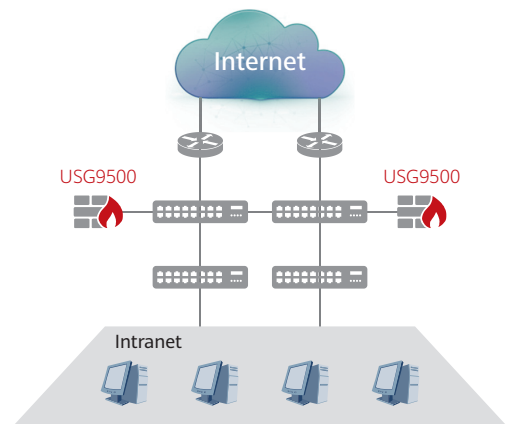
Upgrading data centers to cloud data centers will increase the volume of remote access traffic that a cloud data center handles. Separate security planes are therefore required for different services and tenants; however, deploying traditional security devices at the egress of data centers will complicate internal traffic policing and management and expose data centers to malicious access and attacks. As a result, the functions and performance of traditional security devices at the egress of data centers cannot meet new requirements and have become a bottleneck of data centers.

Solution

As shown in the preceding figure, two USG9500 firewalls are deployed at the ingress of a large IDC/VDC/enterprise network. Virtual systems can be created on the firewalls for different tenants. The bandwidth and number of available sessions of virtual systems can be configured as needed. The virtual systems are isolated from each other, and the external network is isolated from the internal network. Adding SPUs to the USG9500 increases the volume of traffic it can handle, which is more cost-effective than purchasing new devices in terms of per Gigabit power consumption, and also facilitates smooth capacity expansion. The service awareness and log analysis reports provide visibility into network security and forensic evidence. IPS and anti-DDoS boards can be added to block viruses from external networks. To ensure availability and implement millisecond-level switchover, two devices are deployed in active/active or active/standby mode.



USG9500 in In-path Mode



USG9500 in Out-of-path Mode

Hardware

Product Appearance

The USG9500 series comprises the USG9520, USG9560, and USG9580.



USG9520



USG9560






USG9580

By using dedicated multi-core chips and a distributed hardware platform, the USG9500 provides industry-leading service processing and expansion capabilities. Moreover, all key components are redundant to ensure service continuity on high-speed networks, providing a level of availability that is normally seen in core routers. The distributed technology uses line-rate intelligent traffic distribution for data forwarding. All data flows are equally distributed to service processing units (SPUs) to prevent performance bottlenecks. Therefore, the service processing capability increases linearly with service modules, supporting the long-term development of customer networks.




MPU

The USG9500 MPU/SRU has an integrated board structure. It controls the system in a centralized manner and learns routing information. It is the system's control center.

Board	Technical Specification	Mapping Chassis
EKEX16-FWCD00MPUB00 	<ul style="list-style-type: none"> Dimensions (width x depth x height): 398.5 mm x 554 mm x 40.5 mm Maximum power consumption: 95W 	USG9580
E8KE-X8-SRUA-200 	<ul style="list-style-type: none"> Dimensions (width x depth x height): 398.5 mm x 554 mm x 35 mm Maximum power consumption: 160W 	USG9560
E8KE-X3-MPU 	<ul style="list-style-type: none"> Dimensions (width x depth x height): 198.5 mm x 551 mm x 40 mm Maximum power consumption: 35.2W 	USG9520



SPU

The SPUs of the USG9500 process all services. The motherboard of each SPU can hold expansion cards that house multi-core CPUs, which together with the software modules allow the SPUs to process all services on the USG9500. To ensure service continuity, the USG9500 provides SPU redundancy and a heartbeat detection mechanism between the SPU and LPU. If one SPU fails, all functions are switched to other SPUs without interrupting service transmission.

Board	Available slot	Mapping Chassis
X3 Service Processing Unit 2 (Base Board) 	1	USG9520
X8&X16 Service Processing Unit (Base Board) 	2	USG9560 USG9580
Enhanced 20G Firewall Service Processing Unit A 20 	0	USG9520
Enhanced 20G Firewall Service Processing Unit B 20 	0	USG9520
Enhanced 20G Firewall Service Processing Unit A 60&80 	1	USG9560 USG9580
Enhanced 20G Firewall Service Processing Unit B 60&80 	1	USG9560 USG9580

LPU

The USG9500 provides multiple types of I/O interface modules (LPUs) for external connections and data transmissions. Line processing units (LPUs) and SPUs have the same interface slots and can be mixed and matched as needed. The USG9500 provides GE, 10GE, 40GE and 100GE interfaces and supports cross-board port bundling to improve throughput and port density.

Board	Available slot	Mapping FPIC	Mapping Chassis
LPUF-240 	2	<ul style="list-style-type: none">FW-20X1G-RJ45E8KE-X-101-24XGE-SFPE8KE-X-101-5X10GE-SFP+FW-6X10G-SFP+FW-12X10G-SFP+FW-1X100G-CFPFW-3X40G-QSFP+	USG9560 USG9580
LPUF-120 	2	<ul style="list-style-type: none">FW-20X1G-RJ45E8KE-X-101-24XGE-SFPE8KE-X-101-5X10GE-SFP+FW-6X10G-SFP+FW-12X10G-SFP+FW-1X100G-CFPFW-3X40G-QSFP+	USG9520 USG9560 USG9580

Note: for more information, please visit <https://support.huawei.com/enterprise/en/doc/EDOC1100023969?section=j00e&topicName=boards>

Specifications

System Performance and Capacity

Model	USG9520	USG9560	USG9580
IPv4 Firewall Throughput ¹ (1518/512/64-byte, UDP)	120/120/33 Gbit/s	960/960/264 Gbit/s	1,920/1,920/528 Gbit/s
IPv6 Firewall Throughput ¹ (1518/512/84-byte, UDP)	120/120/37 Gbit/s	960/960/296 Gbit/s	1,920/1,920/592 Gbit/s
Firewall Throughput (Packets Per Second)	49Mpps	392Mpps	784Mpps
Firewall Latency (64-byte, UDP)	80 μs	80 μs	80 μs
Security Policies (Maximum)	100,000	100,000	100,000
Virtual Firewalls (Default/Maximum)	10/4,095	10/4,095	10/4,095
URL Filtering: Categories	More than 130		
URL Filtering: URLs	Can access a database of over 120 million URLs in the cloud		

Model	USG9520	USG9560	USG9580
Automated Threat Feed 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 APIs for integration with third-party products through RESTCONF and NETCONF interfaces Other third-party management software based on SNMP, SSH, and syslog Collaboration with third-party tools, such as FireMon Collaboration with Anti-APT solution		
Centralized Management	Centralized configuration, logging, monitoring, and reporting is performed by Huawei eSight and eLog		
VLANs (maximum)	4,094		
Virtual Interfaces (maximum)	1,024		
High Availability Configurations	Active/Active, Active/Standby		

1. Performance is tested under ideal conditions based on RFC 2544 and RFC 3511. The actual result may vary with deployment environments.

Note: This content is applicable only to regions outside mainland China. Huawei reserves the right to interpret this content.

Firewall Service Processing Unit Performance and Capacity

Model	USG9520		USG9560&USG9580	
	Enhanced 20G Firewall Service Processing Unit A 20 (Single CPU)	Enhanced 20G Firewall Service Processing Unit B 20 (Dual CPU)	Enhanced 20G Firewall Service Processing Unit A 60&80 (Single CPU)	Enhanced 20G Firewall Service Processing Unit B 60&80 (Dual CPU)
IPv4 Firewall Throughput ¹ (1518/512/64-byte, UDP)	100/80/16.5	120/120/33	100/80/16.5	120/120/33
IPv6 Firewall Throughput ¹ (1518/512/84-byte, UDP)	100/95/18.5	120/120/37	100/95/18.5	120/120/37
Firewall Throughput (Packets Per Second)	24.5Mpps	49Mpps	24.5Mpps	49Mpps
Firewall Latency (64-byte, UDP)	80 μs	80 μs	80 μs	80 μs
FW + SA* Throughput ²	20 Gbit/s	40 Gbit/s	20 Gbit/s	40 Gbit/s
Concurrent Sessions (HTTP1.1) ¹	80,000,000	160,000,000	80,000,000	160,000,000
New Sessions/Second (HTTP1.1) ¹	800,000	1,600,000	800,000	1,600,000
IPsec VPN Throughput ¹ (AES-256 + SHA2, 1420-byte)	35Gbps	56Gbps	35Gbps	56Gbps
IPsec VPN Throughput ¹ (AES-128 + SHA1, 512-byte)	20Gbps	32Gbps	20Gbps	32Gbps

Model	USG9520		USG9560&USG9580	
	Enhanced 20G Firewall Service Processing Unit A 20 (Single CPU)	Enhanced 20G Firewall Service Processing Unit B 20 (Dual CPU)	Enhanced 20G Firewall Service Processing Unit A 60&80 (Single CPU)	Enhanced 20G Firewall Service Processing Unit B 60&80 (Dual CPU)
Maximum IPsec VPN Tunnels (GW to GW)	64,000	128,000	64,000	128,000
Maximum IPsec VPN Tunnels (Client to GW)	64,000	128,000	64,000	128,000
SSL VPN Throughput ³	2Gbps	4Gbps	2Gbps	4Gbps

1. Performance is tested under ideal conditions based on RFC 2544 and RFC 3511. The actual result may vary with deployment environments.

2. SA performances are measured using 100 KB of HTTP files.

3. SSL VPN throughput is measured using TLS v1.2 with AES128-SHA.

*SA indicates Service Awareness.

Note: This content is applicable only to regions outside mainland China. Huawei reserves the right to interpret this content.

Application Security Service Processing Board Performance and Capacity

Model	Enhanced Application Security Service Processing Card A (Single CPU)	Enhanced Application Security Service Processing Card B (Dual CPU)
SA + IPS Throughput ¹	20 Gbit/s	40 Gbit/s
SA + Antivirus Throughput ¹	18 Gbit/s	36 Gbit/s
SA + IPS + Antivirus + URL Throughput ¹	16 Gbit/s	32 Gbit/s
SA + IPS + Antivirus Throughput (Realworld) ²	14 Gbit/s	28 Gbit/s
SSL Inspection Throughput ³	4.5 Gbit/s	9 Gbit/s

1. Antivirus, IPS, and SA performances are measured using 100 KB of HTTP files.

2. Throughput is measured with the Enterprise Traffic Model.

3. SSL inspection throughput is measured with IPS-enabled and HTTPS traffic using TLS v1.2 with AES256-SHA.

Note: This content is applicable only to regions outside mainland China. Huawei reserves the right to interpret this content.

Hardware Specifications

Model	USG9520	USG9560	USG9580
Dimensions (H × W × D) mm	175 × 442 × 650 (4U, DC) 220 × 442 × 650 (5U, AC)	620 × 442 × 650 (14U)	1420 × 442 × 650 (32U)



Model	USG9520	USG9560	USG9580
Weight (Full Configuration)	Empty: 15 kg (DC) Full configuration: 30.7 kg (DC) Empty: 25 kg (AC) Full configuration: 40.7 kg (AC)	Empty: 43.2 kg Full configuration: 112.9 kg	Empty: 94.4 kg Full configuration: 233.9 kg
Power Supplies	1+1 backup	2+2 backup	4+4 backup
AC Power	90 V AC to 264 V AC; 175 V AC to 264 V AC (recommended)		
DC Power	-72 V to -38 V; -48 V (rated)		
Power Consumption	Typical: 1066W(DC) Typical: 1185W(AC) Most: 1272W(DC) Most: 1414W(AC)	Typical: 4520W(DC) Typical: 4282W(AC) Most: 4823W(DC) Most: 5132W(AC)	Typical: 7387W(DC) Typical: 7858W(AC) Most: 8930W(DC) Most: 9500W(AC)
Working temperature	Extended operation: 0°C to 45°C Storage: -40°C to +70°C		
Ambient humidity	Long term: 5% RH to 85% RH, non-condensing Short term: 5% RH to 95% RH, non-condensing		
Expansion Slot	3	8	16
Maximum Number of Interfaces	12*10GE (RJ45)	96*10GE (RJ45)	192*10GE (RJ45)
Console Ports	2	2	2
Management Ports	2	2	2
MTBF	29.78 years		
MTTR	0.5 hours		

Security Features

Basic Firewall Functions

Transparent, routing, and hybrid modes
Stateful inspection
Blacklist and whitelist

Access control
Application specific packet filter (ASPF)
Security zones

Egress Load Balancing

ISP-based routing
Intelligent uplink selection
Transparent DNS proxy at egress
User-based traffic control
Application-based traffic control
Link-based traffic control
Time-based traffic control

Ingress Load Balancing

Intelligent DNS at ingress
Server load balancing
Application-based QoS

URL Filtering

URL database of 120 million URLs
130+ URL categories
Trend and top N statistics based on users, IP addresses, categories, and counts
Query of URL filtering logs

VPN

DES, 3DES, and AES encryption
MD5 and SHA-1 authentication
Manual key, PKI (X509), and IKEv2
Perfect forward secrecy (DH group)
Anti-replay
Transport and tunnel modes
IPSec NAT traversal
Dead peer detection (DPD)
EAP authentication
EAP-SIM, EAP-AKA
VPN gateway redundancy
IPSec v6, IPSec 4 over 6, and IPSec 6 over 4
L2TP tunnel
GRE tunnel

Anti-DDoS

Prevention of SYN, ICMP, TCP, UDP, and DNS floods
Prevention of port scan, Smurf, teardrop, and IP sweep attacks
Prevention of attacks exploiting IPv6 extension headers
TTL detection
TCP-mss detection
Attack logs

High Availability

Multi-DC cluster

Active/active and active/standby modes
Hot standby (Huawei redundancy protocol)
Configuration synchronization
Data backup between SPUs in a chassis
Firewall and IPSec VPN session synchronization
Device fault detection
Link fault detection
Dual-MPU switchover

Management

Web UI (HTTP/HTTPS)
CLI (console)
CLI (remote login)
CLI (SSH)
U2000/VSM network management system
Hierarchical administrators
Software upgrade
Configuration rollback
STelnet and SFTP

NAT/CGN

Destination NAT/PAT
NAT NO-PAT
Source NAT-IP address persistency
Source IP address pool groups
NAT server
Bidirectional NAT
NAT-ALG
Unlimited IP address expansion
Policy-based destination NAT
Port range allocation
Hairpin connections
SMART NAT
NAT64
DS-Lite
IPv6 rapid deployment (6RD)

Service Awareness

Identification and prevention of over 6000 protocols:
P2P, IM, game, stock charting/trading, VoIP, video, stream media, email, mobile phone services, Web browsing, remote access, network management, and news applications

Antivirus

Detection of 5 million viruses
Flow-based inspection for higher performance
Inspection of encrypted traffic
Trend and top N statistics by virus family



PKI

- Online CA certificate enrollment
- Online CRL check
- Hierarchical CA certificates
- Support for public-key cryptography standards (PKCS#10 protocol)
- CA certificate
- Support for SCEP, OCSP, and CMPv2 protocols
- Self-signed certificates

Intrusion Prevention System

- Protocol anomaly detection
- User-defined signatures
- Automatic update of the knowledge bases
- Zero-day attack defense
- Prevention of worms, Trojan horses, and malware attacks

Networking/Routing

- Support for POS, GE, and 10GE interfaces
- DHCP relay/server
- Policy-based routing
- IPv4/IPv6 dynamic routing protocols, such as RIP, OSPF, BGP, and IS-IS
- Interzone/inter-VLAN routing

Link aggregation, such as Eth-trunk and LACP

Virtual System

- Up to 4095 virtual systems (VSYS)
- VLAN on virtual systems
- Security zones on virtual systems
- User-configurable resources on virtual systems
- Inter-virtual system routing
- Virtual system-specific Committed Access Rate (CAR)
- Separate management of virtual systems
- Resource isolation for different tenants

Logging/Monitoring

- Structured system logs
- SNMPv2
- Binary logs
- Traceroute
- Log server (eLog)

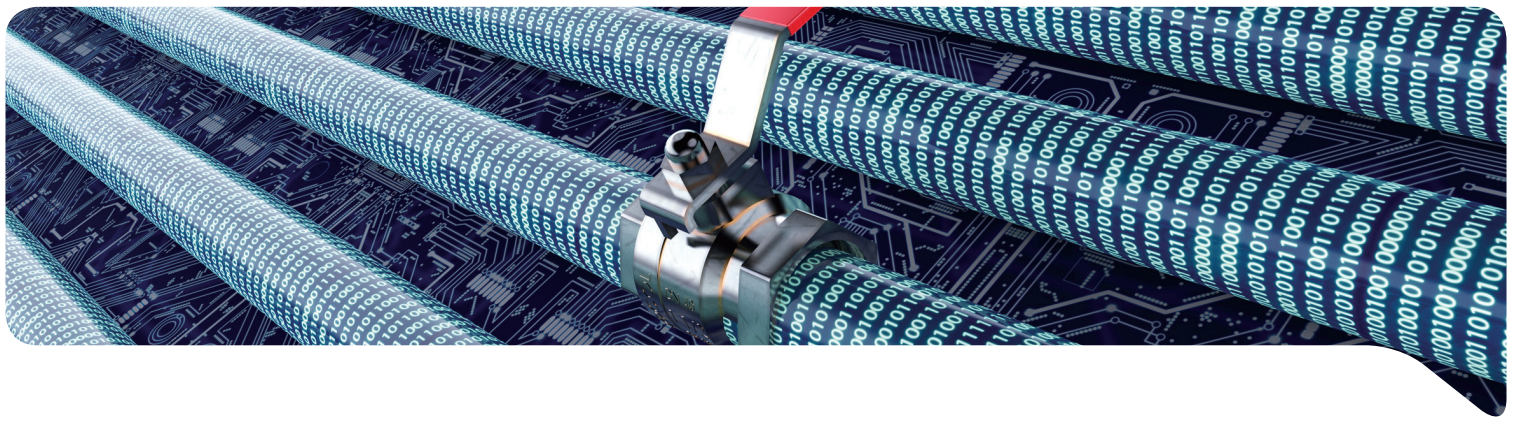
User Authentication and Access Control

- Built-in (internal) database
- RADIUS accounting
- Web-based authentication

Note: Not all versions support all listed features. Contact your Huawei representative for details.

Certifications

Certifications	
Software	ICSA Labs: Firewalls, IPS, IPSec, SLL-TLS, Anti-Virus
Hardware	CB, Rohs, FCC, MET, C-tick, and VCCI



Regulatory, Safety, and EMC Compliance

Certifications	
Regulatory Compliance	Products comply with CE markings per directives 2014/30/EU and 2014/35/EU.
Safety	<ul style="list-style-type: none"> • UL 60950-1 • CSA-C22.2 No. 60950-1 • EN 60950-1 • IEC 60950-1
EMC: Emissions	<ul style="list-style-type: none"> • EN 55022 Class A • ETSI EN 300 386 • IEC 61000-3-2/EN 61000-3-2 • IEC 61000-3-3/EN 61000-3-3 • FCC CFR47 Part 15 Subpart B Class A • ICES-003 Class A • VCCI V-3 Class A • CNS 13438 Class A
EMC: Immunity	<ul style="list-style-type: none"> • EN 55024 • ETSI EN 300 386 • CNS 13438 Class A

Ordering Guide

	Host
USG9520-BASE-AC-51	USG9520 AC Standard Configuration (include X3 AC Chassis, 2*MPU)
USG9520-BASE-DC-51	USG9520 DC Standard Configuration (include X3 DC Chassis, 2*MPU)
USG9560-BASE-DC-51	USG9560 DC Basic Configuration (include X8 DC Chassis, 2*SRU, 1*SFU)
USG9580-BASE-DC-51	USG9580 DC Standard Configuration (include X16 DC Chassis, 2*MPU, 4*SFU)
USG9500 SPUs	
SPU-X8X16-B	X8&X16 Service Processing Unit (Base Board)
SPU-X3-B2	X3 Service Processing Unit 2 (Base Board)
SPUA-20-O-H	Enhanced 20G Firewall Service Processing Unit A 60&80
SPUA-20-O-M	Enhanced 20G Firewall Service Processing Unit A 20
SPCA-20-O-H&M	Enhanced 20G Firewall Service Expansion Card A

	Host
SPUB-20-O-H	Enhanced 20G Firewall Service Processing Unit B 60&80
SPUB-20-O-M	Enhanced 20G Firewall Service Processing Unit B 20
SPCB-20-O-H&M	Enhanced 20G Firewall Service Expansion Card B
SPCA-APPSEC-FW	Enhanced Application Security Service Processing Card A
SPCB-APPSEC-FW	Enhanced Application Security Service Processing Card B
USG9500 LPUs	
FW-LPUF-120	120G Line Processing Unit
FW-LPUF-240	240G Line Processing Unit
FW-6X10G-SFP+	6*10GE SFP+ Daughter Card
FW-1X100G-CFP	1*100GE CFP Daughter Card
FW-12X10G-SFP+	12*10GE SFP+ Daughter Card
FW-3X40G-QSFP+	3-Port 40GBase-QSFP+ Flexible Card
E8KE-X-101-5X10GE-SFP+	5-Port 10GBase LAN/WAN-SFP+ Flexible Card A
FW-20X1G-RJ45	20-Port 10/100/1000Base-RJ45 Flexible Card
E8KE-X-101-24XGE-SFP	24-Port 100/1000Base-X-SFP Flexible Card

Note: This table lists only some parts of the USG9500. For more information, please contact your Huawei representative.

GENERAL DISCLAIMER

The information in this document may contain predictive statement including, without limitation, statements regarding the future financial and operating results, future product portfolios, new technologies, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.

Copyright © 2019 HUAWEI TECHNOLOGIES CO., LTD. All Rights Reserved.