USG9500 Terabit Level Next-Generation Firewall

Product Overview

A fully connected world is becoming a reality. Glasses, watches, and even home appliances and health check products are going smart and digitally connected. In this big data era, the growth of network traffic is exponential, network access methods are diverse, and services can scale on demand.

Mobile working offers convenience, allowing people to be productive at home or anywhere. However, traditional security architectures cannot effectively protect agile and ubiquitous connections from equally ubiquitous vulnerabilities, risks, and intrusions that may compromise data security and privacy. Security has been the top priority in the ICT world.

Therefore, cloud service providers and large data centers and enterprises are upgrading their firewalls at network borders to high-performance and full-featured next generation firewalls (NGFWs). All enterprises that are exploring the viability of mobile working are advised to evaluate the functionality and performance of their firewalls for bottlenecks, and to upgrade their devices before becoming a target of emerging threats.

USG9520

USG9560

USG9580

Product Description

The USG9500 series comprises the USG9520, USG9560, and USG9580, and provides industry-leading security capabilities and scalability. The firewall throughput of the series is up to 1.44 Tbps.

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.

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 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. In addition, the USG9500 provides GE and 10GE interfaces and supports cross-board port bundling to improve throughput and port density.

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 5000 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.
- 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 85 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 1.44 Tbps large-packet throughput, 1.44 billion concurrent connections, and 4096 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.

Specifications

Model	USG9520	USG9560	USG9580
Performance and Capacity			
Maximum firewall throughput*	120 Gbps	720 Gbps	1.44 Tbps
Maximum number of concurrent sessions	120 million	720 million	1.44 billion
Expansion and I/O			
Number of expansion slots	3	8	16
Number of MPU slots	2		
Interface types	GE, 10GE, 40GE, and 100GE interfaces		
SPU	Firewall and application security SPUs		
Dimensions, Power Supply, and Operating Environment			
Dimensions (H x W x D)	175mm x 442 mm x 650 mm (4U, DC) 220 mm x 442 mm x 650 mm (5U, AC)	620 mm x 442 mm x 650 mm (14U)	1420 mm x 442 mm x 650 mm (32U)
Weight	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

Model	USG9520	USG9560	USG9580
Redundant Power Supply	Standard configuration		
AC power supply	90 V AC to 264 V AC; 175 V AC to 264 V AC (recommended)		
DC power supply	–72 V to –38 V; –48 V (rated)		
Power	1270 W	3960 W	7540 W
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 Storage: 0% RH to 95% RH, non-condensing		

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

Security Functions

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

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

URL Filtering

URL database of 85 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

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

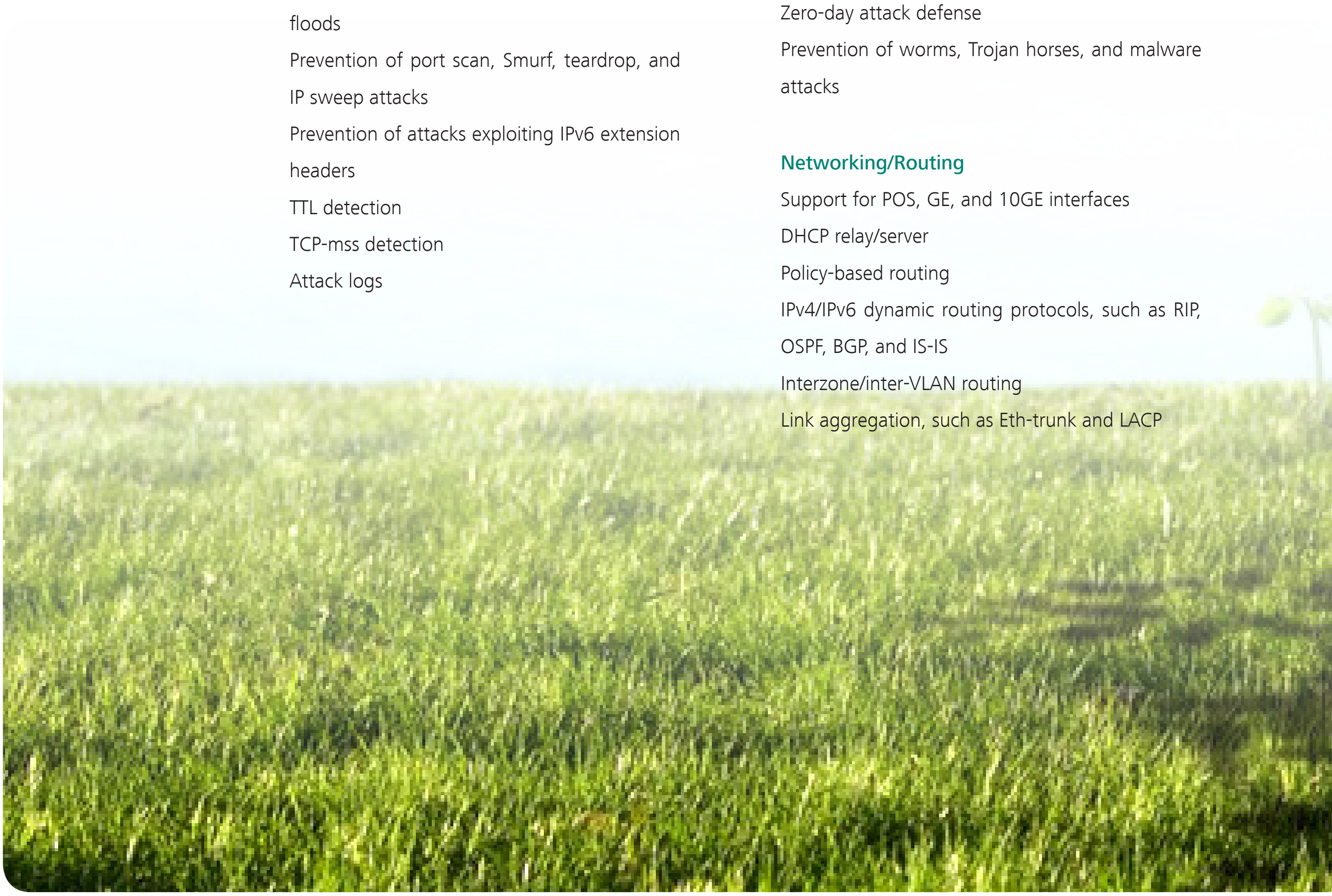
DHCP relay/server

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



High Availability

Active/active and active/standby modes

Hot standby (Huawei redundancy protocol)

Configuration synchronization

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

Certification

Safety certification

Electro Magnetic Compatibility (EMC) certification

CB, Rohs, FCC, MET, C-tick, and VCCI certification

Virtual System

Up to 4096 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

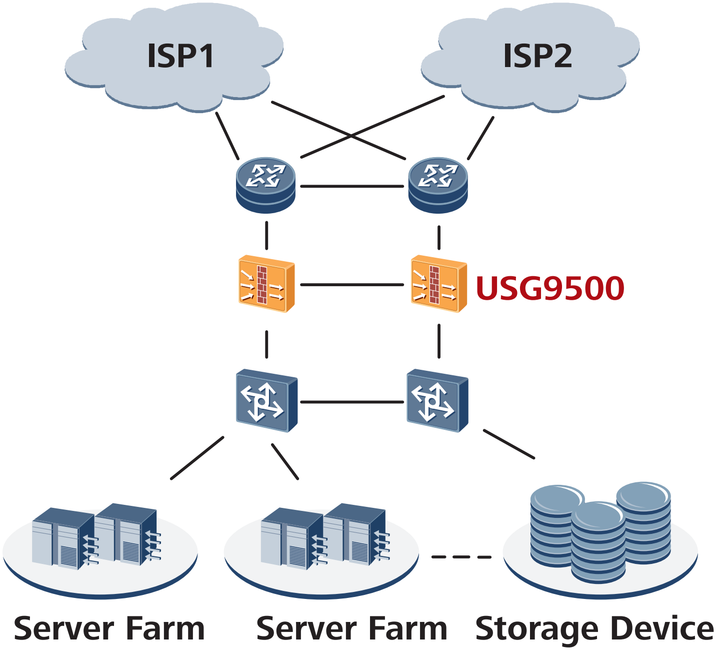
Built-in (internal) database

RADIUS accounting

Web-based authentication

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

Application 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.

Ordering Information

	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-X3-40-E8KE	40G X3 Firewall Service Processing Unit
SPU-X8X16-80-E8KE	80G X8&X16 Firewall Service Processing Unit
SPC-S-40-E8KE	40G Firewall Processing Card
SPC-D-80-E8KE	80G Firewall Processing card
SPC-APPSEC-FW	Application Security Service Processing Card
	USG9500 Flexible Line Processing Units
E8KE-X-LPUF-101	Flexible Card Line Processing Unit(LPUF-101,4 sub-slots)
E8KE-X-101-1X40GE-CFP	1-Port 40GBase LAN CFP Flexible Card(P101,1/2wide,Occupy two sub-slots)
E8KE-X-101-5X10GE-SFP+	5-Port 10GBase LAN/WAN-SFP+ Flexible Card A(P101,1/2wide,Occupy two sub-slots) Spare Part
E8KE-X-101-24XGE-SFP	24-Port 100/1000Base-X-SFP Flexible Card(P101,1/2wide,Occupy two sub-slots)
FW-LPUF-120	120G Line Processing Unit
FW-LPUF-240	Flexible Card Line Processing Unit(LPUF-240,2 sub-slots) Spare Part
FW-6X10G-SFP+	6-Port 10G Base LAN/WAN-SFP+ Flexible Card A Spare Part
FW-1X100G-CFP	1*100GE CFP Daughter Card
FW-12X10G-SFP+	12-Port 10G Base LAN/WAN-SFP+ Flexible Card A(P120-A) Spare Part
E8KE-X-101-1X100GE-CFP	1-Port 100GBase-CFP Integrated Line Processing Unit (LPUI-101)

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