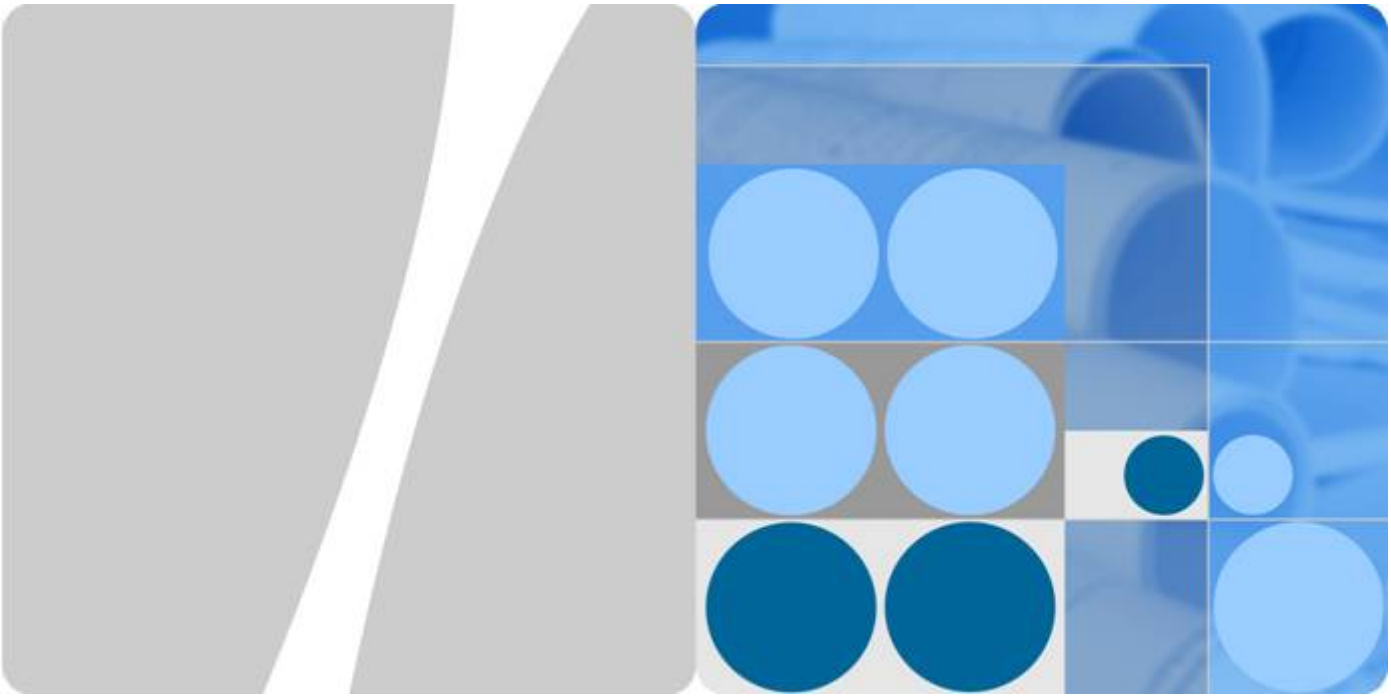


HUAWEI USG9500

V500R001C80

Product Description

Issue 01

Date 2017-11-03

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://e.huawei.com

Contents

1 Introduction....1
1.1 Product Positioning....1
1.2 Highlights....1
2 Application Scenarios....4
2.1 Data Center Border Protection....4
2.2 Tier-2 Carrier Network....5
2.3 Border Protection for Medium- and Large-sized Enterprises....6
2.4 VPN Implementing Branch Interconnection and Mobile Working....8
2.5 Cloud Computing Gateway....9
3 Architecture....10
3.1 Hardware Structure....10
3.1.1 Product Appearance....10
3.1.2 System Configuration....17
3.1.3 Board....18
3.1.4 Physical Hardware Architecture....19
3.1.5 Logical Hardware Architecture....20
3.2 Software Structure....21
3.2.1 Logical Software Architecture....21
3.2.2 Data Forwarding Process....22
4 Functions....24
4.1 USG9500 Functions....24
4.2 Advanced Content Security Defense....30
4.2.1 Accurate Access Control....30
4.2.2 Powerful Intrusion Prevention....32
4.2.3 Refined Traffic Management....33
4.2.4 Perfect Load Balancing....34
5 Operation and Maintenance....37
5.1 Maintenance Features and Functions....37
5.1.1 System Configuration Mode....37
5.1.2 System Management and Maintenance....37
5.1.3 System Service and Status Tracking....38
5.1.4 System Test and Diagnosis....38

5.1.5 Online Upgrade....38
5.1.6 Other Features....38
5.2 Network Management....39
5.3 WEB Configuration and Management....39
5.4 Security....39
6 Technical Specifications....41
6.1 Standards and Protocols....41

1 Introduction

1.1 Product Positioning

ICT transformations in the new era greatly improve enterprise communication efficiency. Devices, such as smartphones and pads, allow people to access the Internet anytime and anywhere and are increasingly used for mobile working. Mobile apps, web 2.0, and social network sites are indispensable on the Internet. Cloud computing enables the rapid service deployment and development and allows on-demand service changes.

However, flexible and various network access modes as well as rapidly increasing service traffic that is computed, stored, or transmitted locally, over pipes, or on clouds consume more bandwidth, overwhelming existing devices. Information explosion brings great challenges and pressures to enterprises' IT systems. From the enterprise information security perspective, mobile working blurs enterprise network borders. Hackers may easily intrude an enterprise IT system through mobile devices. Traditional security gateways defending against attacks based only on IP addresses and ports can hardly cope with ever-changing application and web threats. Information security issues have become complicated.

Huawei USG9500 high-end next-generation firewall is designed to secure network services for cloud service providers, large data centers, and large enterprise campus networks. It provides terabit processing capabilities, integrates multiple security functions, such as NAT, VPN, and virtualization, and delivers 99.999% high availability to meet the ever-increasing high-performance processing requirements on enterprise networks and data centers and minimize equipment room space investment and total cost of ownership (TCO) per Mbps.

The USG9500 series includes the following product models:

- USG9520
- USG9560
- USG9580

1.2 Highlights

Multi-core Distributed Architecture, Maximizing ROI

The USG9500 adopts the NP+multi-core+distributed architecture.

- Each LPU has two network processors (NPs) to provide line rate forwarding.
- The SPU uses multi-core CPUs and a multi-thread architecture to ensure the high speed parallel processing of multiple services.

The SPU and LPU of the USG9500 are independent and can be configured as required. The USG9500 components can be flexibly extended to meet fast increasing service requirements, maximizing ROI for customers.

Industry-Leading High Performance, Ready to Cope With Surging Traffic

The USG9500 provides industry-leading performance:

- The 10-Gigabit line-rate forwarding and the performance of up to 1.92 Tbit/s easily address the challenges brought by the Web 2.0.
- With up to 2560,000,000 concurrent connections and coordinated overall performance with connection quality, the USG9500 is ready to support various Web 2.0 applications.
- With up to 25,600,000 new connections per second, the USG9500 easily meets the challenges of burst problems, such as surging traffic in rush hours and DDoS attacks, to ensure service continuity.

To obtain the specifications of different models, log in to Huawei official website (http://e.huawei.com) and download the product datasheet and specifications lists or contact Huawei engineers.

Full Redundancy and High Availability, Ensuring Service Continuity

The USG9500 provides a comprehensive and reliable end-to-end solution. The high-end router level reliability enables the USG9500 to ensure service continuity.

- Device-level availability
  - Dual-Main Processing Unit (MPU) backup ensures the smooth switchover between MPUs.
  - N+1 backup of Switch Fabric Units (SFUs) enables inter-board data exchange and load balancing.
  - SPUs are load balanced and backed up. If one SPU is faulty, subsequent service traffic will be distributed to other SPUs for processing.
  - The USG9500 has redundant components. In addition, the power modules and fan modules are hot-swappable.
- Network-level availability
  - The USG9500 supports the dual-system hot backup based on the Huawei Redundancy Protocol (HRP), including active/standby backup and load balancing modes. The HRP backs up key configuration commands and the information about session table status from the active device to the standby device. In this manner, the standby device can smoothly take over services when the active device fails.
  - The USG9500 can connect dedicated external bypass devices. When the USG9500 is faulty, network traffic can be forwarded by the Bypass device in a timely manner to ensure service continuity.
- Link-level availability
  - The USG9500 supports cross-board interface binding to enable balanced traffic forwarding, improve link availability, and broaden the total bandwidth.

- The USG9500 supports Bidirectional Forwarding Detection (BFD) to rapidly detect and monitor the connectivity of links or IP routes.

2 Application Scenarios

2.1 Data Center Border Protection

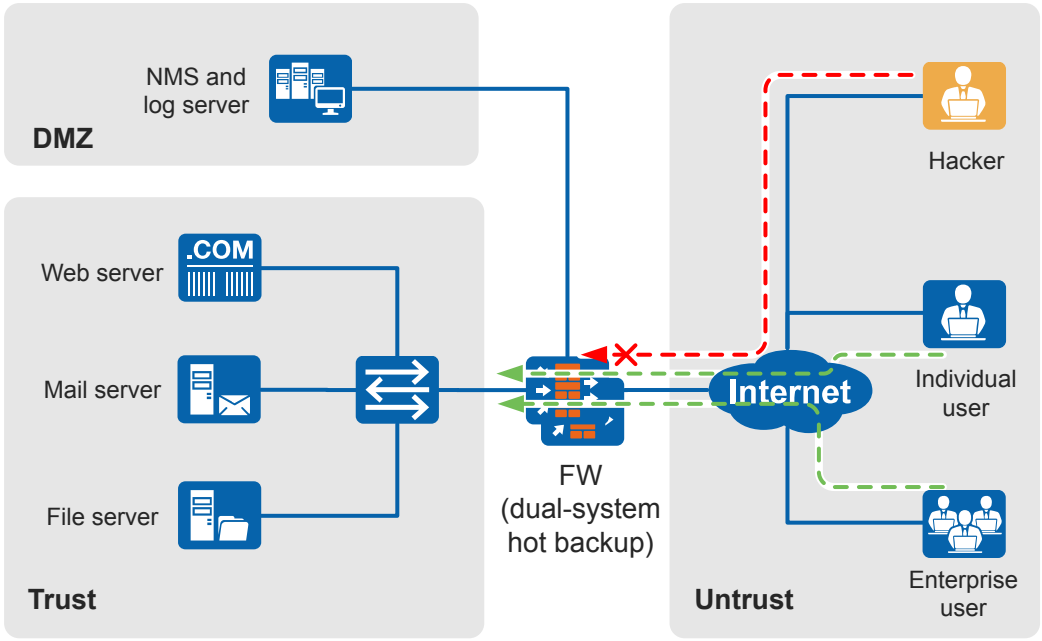
Internet Data Center (IDC) is an infrastructure that involves maintenance services to collect, store, process, and send data on the Internet. The IDC is constructed by a network server provider to provide the server hosting and virtual domain name services for small and medium-sized enterprises and individual customers.

The network structure of the IDC has the following features:

- Provides network services for external users, which is the key function of the IDC. The normal access from the Internet to servers in the IDC must be guaranteed. Therefore, the border protection device must have high performance and reliability and ensure network access when attacks are launched on the IDC.
- Protects servers in the IDC and applies security functions according to the service type.
- May deploy servers of multiple enterprises in an IDC and are easily targets for hackers.
- The IDC traffic is complex. The administrator cannot effectively adjust configurations if the traffic is not clear.

The USG9500 works as the border gateway of an IDC to cope with the previous issues. **Figure 2-1** shows the typical application scenario.

Figure 2-1 Typical networking of data center border protection



You can set up border protection for data centers as follows:

- Use SLB and smart DNS to evenly and properly distribute traffic accessing one server group and prevent server overload and idleness.
- Apply traffic limiting on the basis of the IP address and application to ensure the stable operating of servers and avoid network congestion.
- Enable the intrusion prevention and antivirus functions to protect servers from viruses, Trojan horses, and worms.
- Enable the anti-DDoS and other attack defense functions to defend against attacks from the Internet.
- Deploy the eSight network management system (to be purchased independently) to log the network operating. The logs help the administrator adjust configurations, identify risks, and check traffic.
- Deploy the dual-system hot backup network to improve availability. When a single-point failure occurs, service traffic can be smoothly switched from the active device to the standby device to ensure continuity.

2.2 Tier-2 Carrier Network

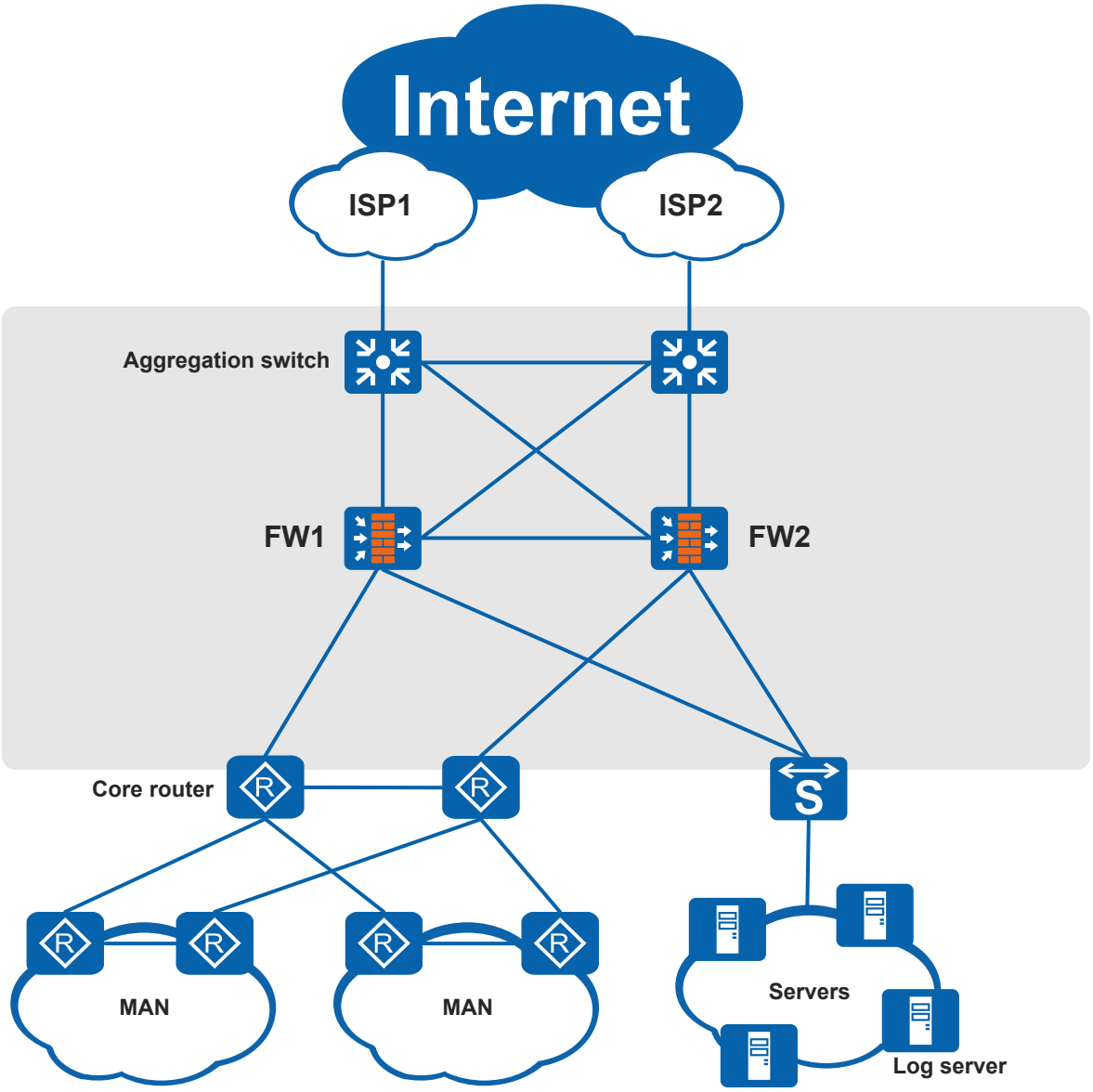
This section describes how the USG9500 protects tier-2 carrier networks.

Tier-2 carrier networks are increasingly popular these days. Generally, a tier-2 carrier network face the following challenges:

- Connected to different ISPs at different prices, with unevenly distributed traffic.
- Suffered low bandwidth efficiency due to P2P traffic.
- URL source tracing is required.

Based on the preceding challenges, **Figure 2-2** shows a typical application of the USG9500 on a tier-2 carrier network.

Figure 2-2 Typical deployment of a tier-2 carrier network



- Automatic selection of an optimal uplink based on applications, routes, users, time, and links reduces unnecessary bandwidth consumption.
- P2P intranet acceleration saves public network bandwidth.
- The many-to-one NAT server saves hardware investment, improves bandwidth efficiency, and reduces bandwidth costs.
- A log system is used to trace the sources of NAT addresses and URL addresses.

2.3 Border Protection for Medium- and Large-sized Enterprises

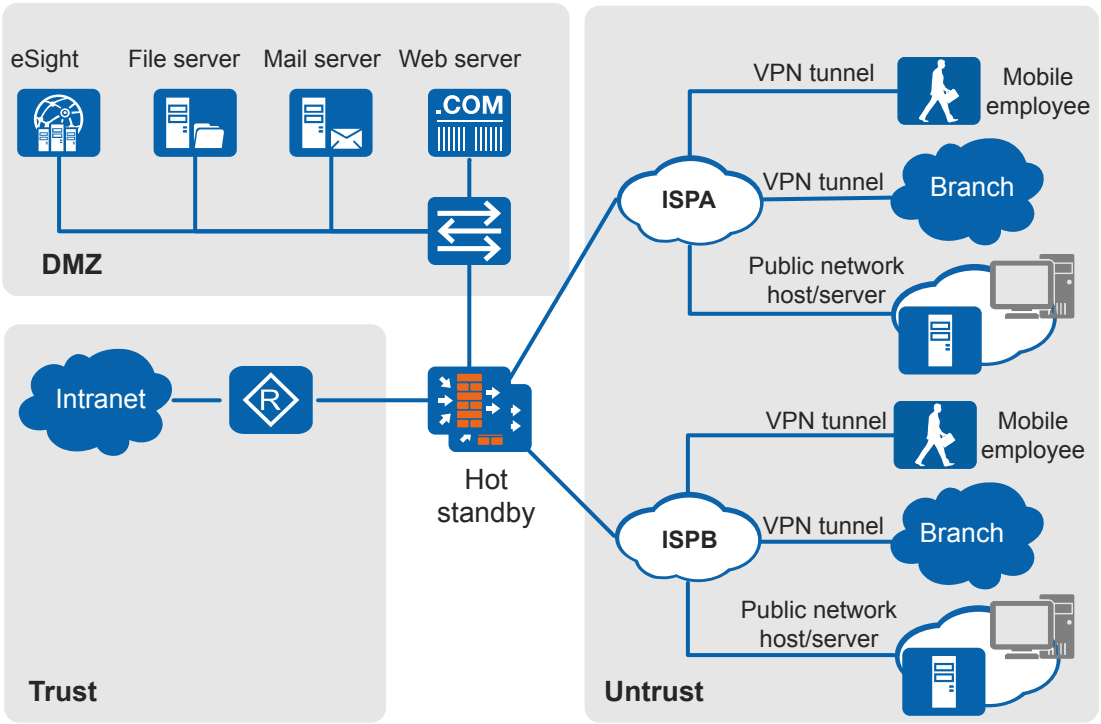
This section describes how to use the USG9500 as the egress gateway of a medium- or large-sized enterprise to ensure network security.

The medium- or large-sized enterprise has the following service features:

- High requirements on device reliability for service continuity when traffic is heavy or the device is faulty
- Large number of employees, complex services, and various flows
- Services available to external users, for example, the website and mail services
- Exposure to DDoS attacks and great losses after the attacks succeed

The USG9500 works as the egress gateway of a medium- or large-sized enterprise to cope with the issues listed in this section. **Figure 2-3** shows the typical application scenario.

Figure 2-3 Typical networking of border protection for large and medium-sized enterprises



- Use ISP link selection, intelligent uplink selection, and transparent DNS to properly allocate outbound link bandwidth, forward traffic efficiently, and prevent traffic diversion and single-link congestion.
- Apply bandwidth policies to traffic between the intranet and the Internet to control the bandwidth and number of connections to avoid network congestion and defend against DDoS attacks.
- Establish VPN tunnels between the USG9500, mobile workers, and branches to protect service data during the transmission over the Internet.
- Enable the anti-DDoS function to defend against heavy-traffic attacks launched by the Internet hosts to ensure the normal operating of services.
- Deploy the eSight network management system (to be purchased independently) to log the network operating. The logs help the administrator adjust configurations, audit traffic and identify risks.
- Deploy the dual-system hot backup network to improve availability. When a single-point failure occurs, service traffic can be smoothly switched from the active device to the standby device to ensure continuity.

2.4 VPN Implementing Branch Interconnection and Mobile Working

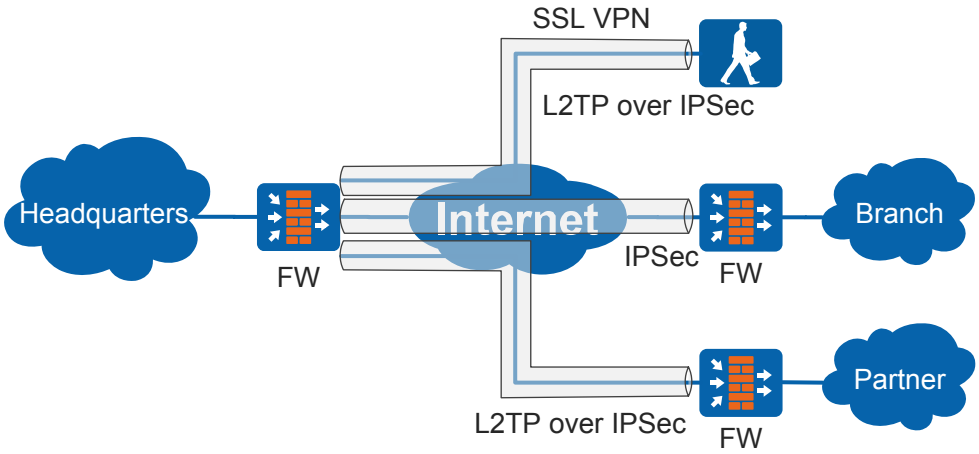
To develop services globally, enterprises may set branches or cooperate with institutes in other places. Employees in branches, mobile employees or partners need to remotely access the headquarters. Currently, the VPN technology can be used to achieve secure and low-cost remote access.

Remote access and mobile working have the following features:

- Branches need access to the headquarters and continuously develop services.
- Partners must be flexibly authorized to limit the accessible network resources and transmittable data types according to the services.
- Employees on the move need to be connected anywhere, anytime, and at any IP address. In addition, employees on the move are not protected by information security measures. Enterprises must implement strict access authentication on these employees and accurately control their accessible resources and permissions.
- Enterprises must implement encryption protection on data transferred during remote access communications to prevent network eavesdropping, tampering, forgery, and replay as well as information leaks.

The USG9500 works as the VPN access gateway of an enterprise to cope with the issues listed in this section. **Figure 2-4** shows the typical application scenario.

Figure 2-4 Typical networking of VPN remote access and mobile working



- Establish IPSec or L2TP over IPSec permanent tunnels for the branches and partners with fixed VPN gateways. If access account verification is required, the L2TP over IPSec tunnel is recommended.
- Apply SSL VPN technologies to employees on the move (with unfixed addresses). The VPN client installation is not required. These employees can use only web browsers to establish tunnels with the headquarters, which is convenient. Meanwhile, resources accessible to the employees on the move are controlled in a refined manner, or use L2TP over IPSec to establish an IPSec tunnel with the headquarters.
- Use the IPSec or SSL encryption algorithm to protect network data in the previous tunnels.

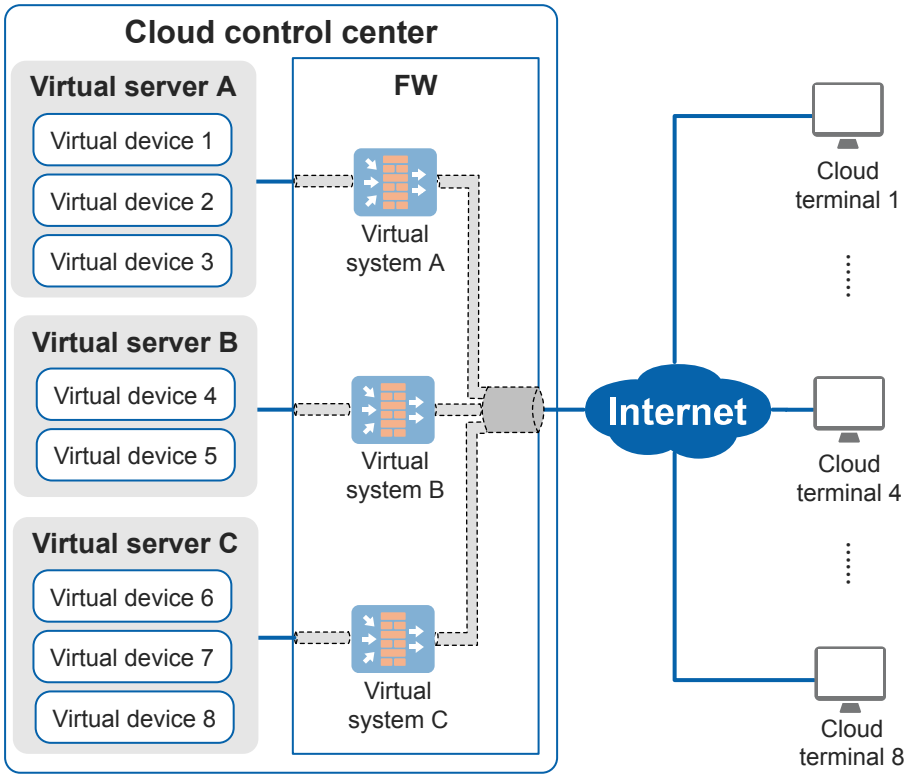
- Apply access authentication on the access users of VPN tunnels to ensure user legitimacy and apply access authorization on the basis of user permissions.
- Enable the intrusion prevention and anti-DDoS functions to prevent remote access users from introducing network threats as well as information leaks.

2.5 Cloud Computing Gateway

Cloud computing has multiple applications. Typically, an ISP provides hardware resources and computing capabilities for users. Each user can use only one terminal to access the cloud, similar to operating a PC.

The core technology of cloud computing provides independent and complete services for a large number of users based on the server cluster, which involves multiple virtualization technologies. The FW works as the cloud computing gateway. **Figure 2-5** shows a typical application scenario.

Figure 2-5 Typical networking of cloud computing



In this scenario, the FW is the cloud computing gateway. The system virtualization function divides a physical device into multiple independent logical devices. Each logical device, called a virtual system, has its own interface, system resource, and configuration file and implements traffic forwarding and security detection independently.

Virtual systems are logically isolated. Therefore, each cloud terminal seems to have an exclusive firewall. These virtual systems share the same physical entity, and traffic forwarding between virtual systems is highly efficient. In this scenario, the FW is used for the rapid data switching among virtual systems, protects traffic between cloud terminals and the cloud server, and provides value-added security services for cloud computing.

3 Architecture

3.1 Hardware Structure

3.1.1 Product Appearance

The USG9500 uses an integrated chassis. The chassis can be installed in an N68E-22 cabinet or a standard International Electrotechnical Commission (IEC) 19-inch cabinet with a depth no less than 800 mm.

USG9520 Chassis Overview

The USG9520 chassis have both AC and DC models. **Figure 3-1** shows a DC chassis, and the **Figure 3-2** shows an AC chassis.

Figure 3-1 Appearance of a DC chassis

Figure 3-2 Appearance of an AC chassis

Figure 3-3 shows the slot layout of the USG9520.

Figure 3-3 Slot layout on the USG9520

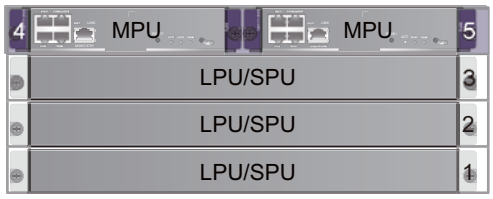


Table 3-1 Table 1 Board distribution in the board cage of the USG9520

Slot Name	Slot Number	Quantity	Slot Height	Remarks
LPU/SPU	1 to 3	3	41 mm (1.6 inches)	These slots are used to hold LPUs or SPUs.
MPU	4 to 5	2	41 mm (1.6 inches)	These slots hold MPUs that work in 1:1 backup mode.

USG9560 Chassis Overview

Figure 3-4 shows the chassis of the USG9560.

Figure 3-4 Appearance of the chassis of the USG9560

Figure 3-5 shows the slot layout of the USG9560.

Figure 3-5 Slot layout on the USG9560

Table 3-2 Table 1 Board distribution in the board cage of the USG9560

Slot Name	Slot Number	Quantity	Slot Height	Remarks
LPU/SPU	1 to 8	8	41 mm (1.6 inches)	These slots are used to hold LPUs or SPUs.

Slot Name	Slot Number	Quantity	Slot Height	Remarks
SRU	9 to 10	2	36 mm (1.4 inches)	These slots hold SRUs that work in 1:1 backup mode.
SFU	11	1	36 mm (1.4 inches)	These slots are used to hold an SFU.

USG9580 Chassis Overview

Figure 3-6 shows the chassis of the USG9580.

Figure 3-6 Appearance of the chassis

Figure 3-7 shows the slot layout of the USG9580.

Figure 3-7 Slot layout on the USG9580

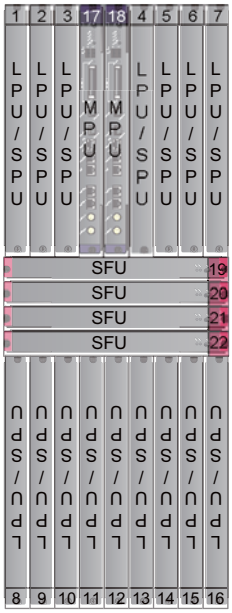


Table 3-3 Table 1 Board distribution in the board cage of the USG9580

Slot Name	Slot Number	Quantity	Slot Height	Remarks
LPU/SPU	1 to 16	16	41 mm (1.6 inches)	These slots are used to hold LPUs or SPUs.
MPU	17 to 18	2	41 mm (1.6 inches)	These slots hold MPUs that work in 1:1 backup mode.
SFU	19 to 22	4	41 mm (1.6 inches)	These slots are used to hold SFUs.

Power and Heat Dissipation Systems of the USG9500

Table 3-4 shows the overview of the power supply and heat dissipation systems of the USG9500 of different models.

Table 3-4 Overview of the power supply and heat dissipation systems of the USG9500 of different models

Component	USG9520	USG9560	USG9580
Power supply system	Supports AC or DC power supplies.		

Component	USG9520	USG9560	USG9580
	The power supply system consists of 1+1 redundant AC or DC power supply frames. Both the AC and DC power supply frames support power alarming.	● In DC mode, four Power Entry Modules (PEMs) reside on the back panel to provide 2+2 backup. ● In AC mode, an AC power supply frame resides externally and connects to the power input ports of the PEMs through a rectifier that suits the total power of the integrated chassis.	● In DC mode, eight PEMs reside on the back panel to provide 4+4 backup. ● In AC mode, two AC power supply frames reside externally and connect to the power input ports of the PEMs through a rectifier that suits the total power of the integrated chassis.

Component	USG9520	USG9560	USG9580
Heat dissipation system	● Air enters the chassis from the left and exits from the back. ● The air intake vent is on the left of the chassis, and the air exhaust vent is on the back of the chassis. ● The fans reside on the air exhaust vent. The two fan frames back against each other, and each has two fans. The fan frame extracts air from the system for dissipation.	● Air enters the chassis from the front and exits from the back. ● The air intake vent is above the front board slot area, and the air exhaust vent is above the rear board slot area. ● The fans reside on the air exhaust vent. The two fan frames back against each other. Each fan frame has one fan. The fan frame extracts air from the system for dissipation.	● The two fan frames reside respectively on the upper and lower parts of the chassis. Air enters the chassis from the front and exits from the back. ● For the upper fan frame, the air intake vent resides above the front board slot area, and the air exhaust vent resides above the rear board slot area. For the lower fan frame, the air intake vent resides above the rear board slot area, and the air exhaust vent resides above the front board slot area. The upper and lower fan frames function independently. ● The board slot area for the SFU resides on the middle part of the device. The area intake vent for this slot area is on the left of the chassis. To dissipate the SFUs in the two upper slots, the air enters from the left and goes up on the right to converge with the air from the upper fan frame. To dissipate the SFUs in the two lower slots, the air enters from the left and goes down on the right to converge with the air

Component	USG9520	USG9560	USG9580
			from the lower fan frame.

3.1.2 System Configuration

Table 3-5 lists the system configuration of the FW series.

Table 3-5 FW series system configuration

Item	USG9520	USG9560	USG9580	Remarks
CPU processing capability on the MPU	Main frequency: 1 GHz	Main frequency: 1.5 GHz	Main frequency: 1.5 GHz	-
BootROM capacity of the MPU	1 MB	8 MB	8 MB	-
SDRAM capacity of the MPU	2 GB	4 GB	4 GB	-
NVRAM capacity of the MPU	512 KB	4 MB	4 MB	-
Compact Flash (CF) card	2x2GB	2x2GB	2x2GB	-
Number of MPU slots	2	2	2	1:1 backup
Number of SFU slots	-	1	4	● The independent SFUs on the USG9560 interwork with the SFU integrated on the SRU to form 2+1 backup for load balancing. ● The independent SFUs of the USG9580 form 3+1 backup for load balancing.

Item	USG9520	USG9560	USG9580	Remarks
Number of LPU slots	3	8	16	Each LPU slot can house an SPU. In normal cases, the SPU and the LPU need to be configured in accordance with the closest capacity.
Switching capacity	1.35 Tbit/s	15 Tbit/s	30 Tbit/s	Bidirectional
Maximum port rate	100Gbit/s			

3.1.3 Board

Main Processing Unit (MPU)

The MPU on the FW is in charge of system control and route information learning. It is the central control unit of the device.

The FW MPU uses the 1:1 backup mechanism. When the active MPU is faulty, the standby MPU immediately takes over the work. The backup mechanism ensures the proper running of services.

Switch Fabric Unit (SFU)

The SFU in the FW is in charge of data exchange among boards.

- The USG9560 is equipped with three SFUs, two of which, together with two MPUs, are integrated on respectively two SRUs. The third SFU works independently.
  - Enables 2+1 load balancing backup in the switching network.
  - Three SFUs work simultaneously to share the service data. When one of them is faulty, the service data is automatically balanced to the other two without interrupting services.
- The USG9580 equips with four SFUs.
  - Enables 3+1 load balancing backup in the switching network.
  - Four SFUs work simultaneously to share the service data. If any SPU is faulty, the service data is automatically balanced to the other three without interrupting services.

Service Processing Unit (SPU)

The SPU of the FW is in charge of security service processing.

The SPU of the FW comes with high-performance multi-core central processing units (CPUs). A service processing card (SPC) or two SPCs can be installed on each SPU.

The FW can house multiple SPUs. If multiple SPUs are used, The system performance in terms of the throughput and the number of new connections per second will increase in a linear fashion. The SPUs support mutual backup. When one SPU is faulty, all its traffic is immediately balanced to other SPUs without interrupting services.

Line Processing Unit (LPU)

FW supports the following LPUs:

- LPUF-240

  The LPUF-240 which enhances networking flexibility and provides low-cost and customized solutions supports packet forwarding at the line speed of 240 Gbit/s. The LPUF-240 provides two 1/2-width slots, and each slot holds one FPIC. The LPUF-240 supports mixed insertion between different FPICs. The LPUF-240 cannot be used on the USG9520 platform.
- LPUF-120

  The LPUF-120 which enhances networking flexibility and provides low-cost and customized solutions supports packet forwarding at the line speed of 240 Gbit/s. The LPUF-120 provides two 1/2-width slots, and each slot holds one FPIC. The LPUF-120 supports mixed insertion between different FPICs.
- LPUF-101

  The LPUF-101 which enhances networking flexibility and provides low-cost and customized solutions supports packet forwarding at the line speed of 100 Gbit/s. The LPUF-101 provides four 1/4-width slots or two 1/2-width slots, and each slot holds one FPIC. The LPUF-101 supports mixed insertion between different FPICs.

3.1.4 Physical Hardware Architecture

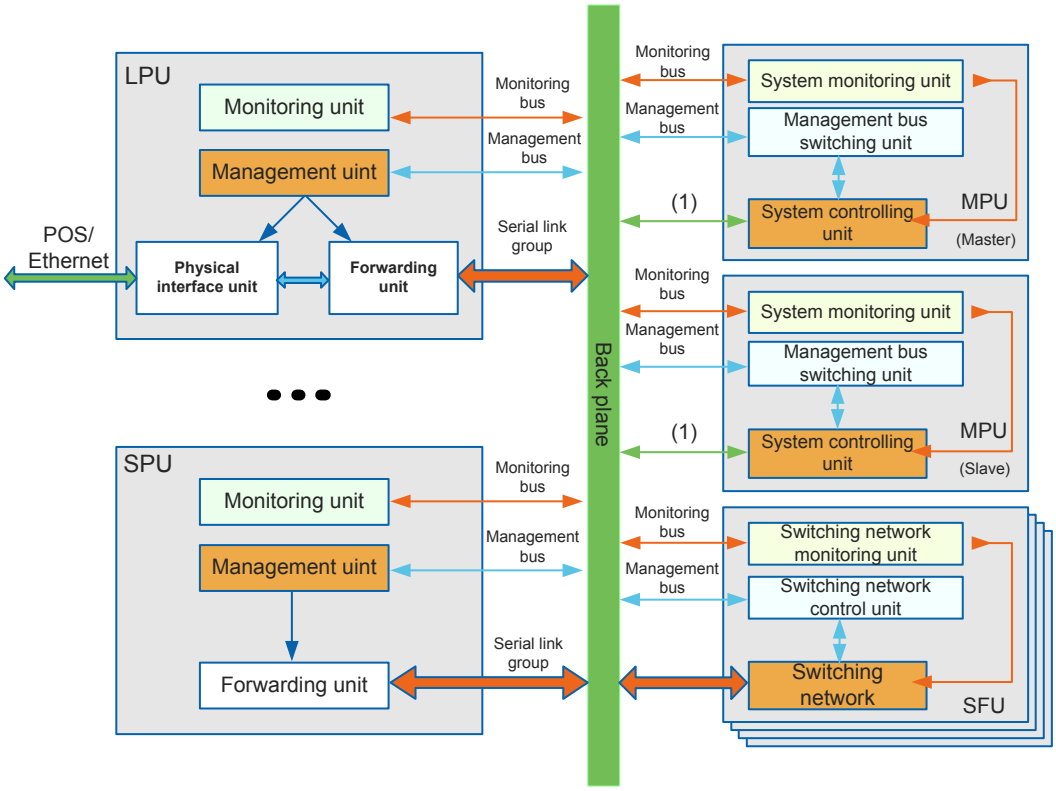
The USG9500 consists of the following subsystems:

- Power supply system
- Heat dissipation system
- Functional host system
- Network Management System (NMS)

Except the NMS, all subsystems locate in the integrated chassis.

- The NMS, independently deployed on the server, is used to configure and manage the USG9500.
- For details on the functions of the power supply system (in 1+1 backup mode) and the heat dissipation system, see **FW Power Supply and Heat Dissipation Systems**
- The functional host system consists of system backplane, MPU, LPU, SPU, and SFU. This system mainly performs data processing. In addition, the system monitors and manages all devices in the system, including power modules and fan modules. The functional host system connects to the NMS through the NMS interface. **Figure 3-8** shows the diagram of the functional host.

Figure 3-8 Diagram of the functional host



(1) The link connects to the management bus switching unit of another

NOTE

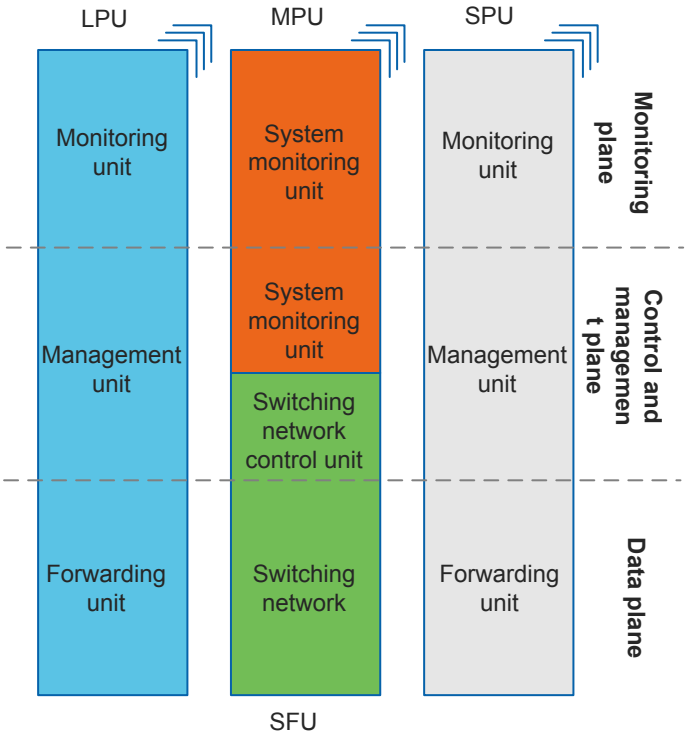
Figure 3-8 applies only to the USG9560 and USG9580. The USG9520 uses the Full Mesh architecture and has no SFU.

3.1.5 Logical Hardware Architecture

The logical architecture of the USG9500 consists of the following planes:

- Data plane
- Control and management plane
- Monitoring plane

Figure 3-9 Diagram of logical hardware architecture



- The data plane is responsible for high speed processing and non-blocking switching of data packets. It encapsulates or decapsulates packets, processes security services, forwards IPv4/IPv6 packets, performs QoS and scheduling, completes inner high-speed switching, and collects statistics.
- The control and management plane is the core of the entire system. It controls and manages the system. The control and management plane processes protocols and signals, configures and maintains the system status, and reports and controls the system status.
- The monitoring plane monitors the system environment. It detects the voltage, controls the power-on and power-off of the system, monitors the temperature, and controls the fan. In this manner, the security and stability of the system are ensured. The monitoring plane helps isolate the fault promptly in the case of faults to guarantee the operation of other parts.

The USG9500 is based on the dedicated modular security software platform and completely separates the forwarding and control functions. The control function of the USG9500 is based on the MPU whereas the forwarding function is based on the LPU and SPU.

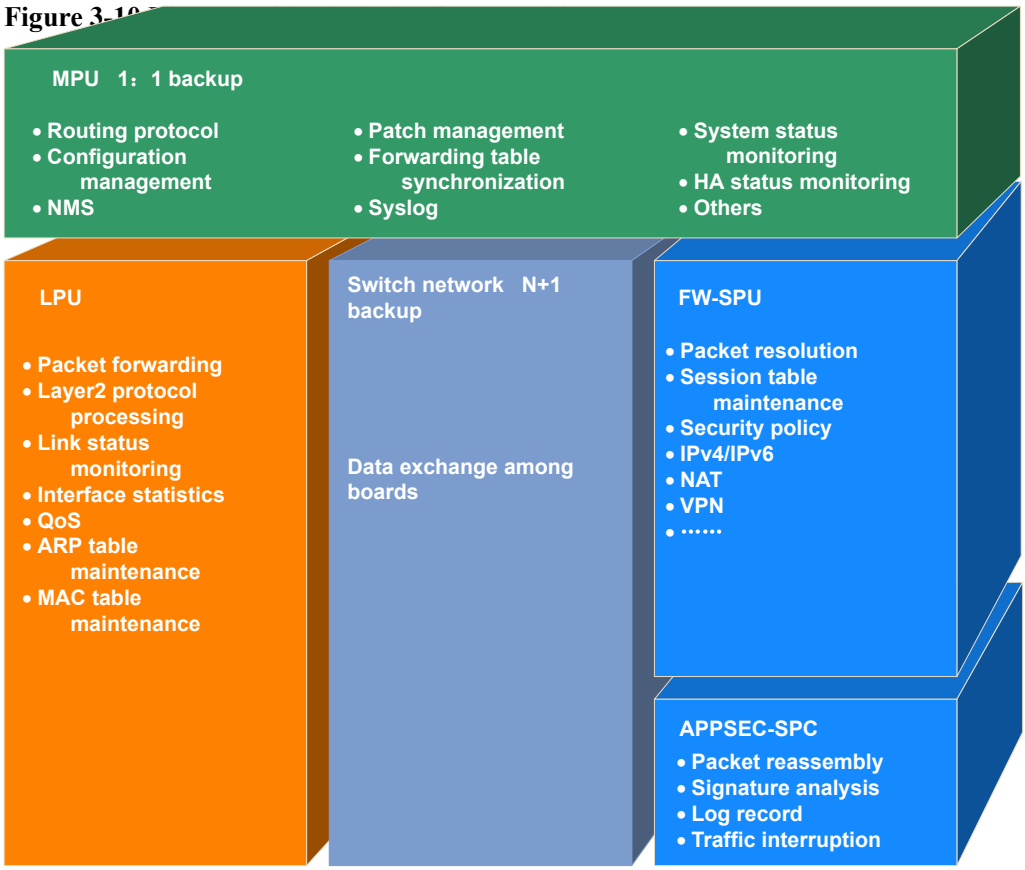
3.2 Software Structure

3.2.1 Logical Software Architecture

The USG9500 uses the flexible and mature versatile routing platform (VRP). Based on the component technology, the VRP supports the distributed architecture and improves security features and reliability.

Figure 3-10 shows the logical diagram of the software architecture.

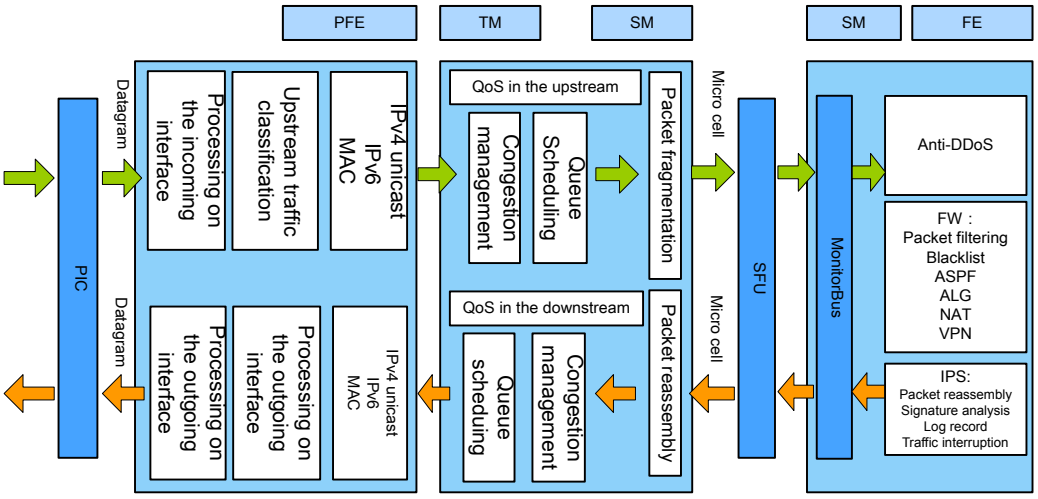
Figure 3-10



3.2.2 Data Forwarding Process

FW shows the data forwarding flowchart.

Figure 3-11 Data forwarding flowchart



Based on data directions, data forwarding is divided into three phases: upstream processing, SPU processing, and downstream processing.

- Upstream processing

  A packet is encapsulated in a frame on the Physical Interface Card (PIC) and then sent to the Packet Forwarding Engine (PFE). On the incoming interface, the packet is decapsulated and the packet type is identified. Then, traffic is classified according to the configurations on the incoming interface. Subsequently, scheduling priorities are generated and added to the packet. Then the packet is sent to the Traffic Manager (TM) where the scheduling for Quality of Service (QoS) is completed.

- SPU processing

  After the upstream process in the LPU, the SFU sends the packet to the forwarding engine in the SPU. Then the forwarding engine searches the session table. If a match is found, the packet is sent for security processing based on the matched session entry. If no match is found, the packet is the first packet of the session. The forwarding engine searches the Forwarding Information BASE (FIB) based on the destination IP address of the packet. By searching the FIB, the forwarding engine obtains the outbound interface and the next hop of the packet, and then sends the packet for security processing, such as packet filtering and content security checks.

- Downstream processing

  After the processing in the SPU is complete, the packet is sent through the SFU to the downstream LPU. In the LPU, the packet is processed for downstream QoS and downstream traffic classification. Finally, based on the configurations on the outgoing interface, the packet is encapsulated with the new Layer-2 header and is then sent to the PIC.

4 Functions

4.1 USG9500 Functions

This section describes the main functions supported by the USG9500.

Table 4-1 USG9500 functions

Category	Function	Description
Content Security	Application identification	● Identifies common applications based on the predefined signature database. ● Supports the constant update of the predefined signature database and the user-defined applications. ● Parses the packets of tens of protocols and identifies the contents during the protocol negotiation and supports common multi-channel protocols.
	SSL-Encrypted Traffic Detection	Decrypts SSL traffic and implements content security check on verified traffic.
	Antivirus	● Employs the advanced Intelligent Awareness Engine (IAE) and constantly updated virus signature database to detect and remove viruses. ● Updates the signature database constantly.
	Intrusion prevention	● Detects and defends against thousands of common intrusion behaviors, worms, Trojan horses, and botnets. ● Updates the predefined signature database constantly and supports user-defined signatures.

Category	Function	Description
	URL filtering	● Blocks connections to HTTP and HTTPS URLs as required. ● Adds URLs and URL categories on the local and supports the query of the latest URLs and URL categories from the URL remote query server. ● Updates URL categories constantly.
	DNS Filtering	Supports the DNS filtering function, which filters domain names in DNS requests at the domain name resolution stage to control operating or accessible websites.
	Data filtering	● Supports common file transfer protocols, including HTTP, FTP, SMTP, POP3, NFS, SMB, IMAP, RTMPT, and FLASH. ● Filters contents in the files transferred over the previous protocols based on keywords. ● Filters contents in the HTTP and FTP files based on keywords.
	File blocking	● Supports common file transfer protocols, including HTTP, FTP, SMTP, POP3, NFS, SMB, IMAP, RTMPT, and FLASH. ● Identifies common documents, code files, executable files, multimedia files, real types of the compressed files, and file name extensions over the previous protocols. ● Identifies common files transferred over the previous protocols based the real types and file name extensions.
	Application behavior control	● Controls HTTP behaviors, including the file upload and download, POST, web page browsing, and HTTP proxy. ● Controls FTP behaviors, including FTP file upload and download.
	Mail filtering	● Supports the mail server whitelist and blacklist on the local to block the spam. ● Works with the RBL server to remotely query whether a mail is spam in real time. ● Filters mails based on the sender addresses, receiver addresses, and the size and number of mail attachments.
	Anti-APT	Interworks with a sandbox to detect and defend against APT attacks.

Category	Function	Description
User management	Local user management	● Supports user creation and management and organization structure maintenance. ● Supports centralized management of VPN users.
	Interworking the user server	Interworks with common user servers such as AD, RADIUS, HWTACACS, LDAP, SecurID, and Agile Controller to import user information and implement proxy authentication.
	User authentication	Pushes web pages for user authentication or works with the AD server to, in real time, synchronize information about online users.
Network-Layer Security Protection	Packet filtering	Supports packet filtering based on policies.
	NAT	● Translates the source IP addresses, destination IP addresses, and ports of packets. ● Maps private IP addresses and ports to public IP addresses and ports, so that the internal server can provide services for external users. ● Automatically translates the IP addresses and ports negotiated in the packets of common multi-channel protocols.
	CGN	Provides the NAT444 function to deploy NAT twice at both the enterprise gateway and carrier egress. Employs the PCP technology, which is based on P2P, to enable such services as file sharing, voice communication, and video transmission to run properly in NAT444 scenarios. Provides the static mapping function in NAT444 scenarios for quick tracing of user addresses. Provides the DS-Lite function to combine tunneling and NAT, allowing private IPv4 users to traverse the IPv6 network to access the IPv4 Internet. Supports port pre-allocation and incremental allocation. The port range is pre-allocated before NAT for a user, so subsequent services from this user will use this port range for processing. Employs the NAT64 technology to enable IPv4 and IPv6 networks to communicate.
	DDoS attack defense	Defends against various DoS and DDoS attacks: ● Non-application-layer DDoS attacks: SYN flood, UDP flood, ICMP flood, and ARP flood ● Application-layer DDoS attacks: HTTP flood, HTTPS flood, DNS flood, and SIP flood

Category	Function	Description
	Single-packet attack defense	Implements packet validity checking to defend against various single-packet attacks, including IP spoofing attacks, LAND attacks, Smurf attacks, Fraggle attacks, Winnuke attacks, Ping of Death attacks, Teardrop attacks, address scanning attacks, port scanning attacks, IP option control attacks, IP fragment control attacks, TCP label validity check attacks, ICMP packet control attacks, ICMP redirect packet attacks, ICMP unreachable packet attacks, and TRACERT packet attacks.
	IP reputation database-based security protection	Filters packets based on zombie hosts' IP addresses recorded in the IP reputation database.
	Blacklist	Rapidly filters packets based on the blacklist of IP addresses.
	IP-MAC address binding	Supports IP-MAC address binding to prevent IP spoofing.
	CIS Interworking	Supports interworking between the FW and CIS system. After the CIS detects a malicious session based on analysis and delivers a blocking command to the FW, the FW deletes the session and blocks the traffic matching the session.
	SCTP	Supports the configuration of SCTP NAT.
Traffic Management	IP address- and user-based bandwidth management	Limits the maximum bandwidth and guaranteed bandwidth for an IP address or a user.
	IP address- and user-based connection quantity management	Limits the maximum number of connections for an IP address or a user.
	Interface-based bandwidth management	Limits the maximum bandwidth for an interface.
Intelligent Uplink Selection	Smart DNS	Modifies DNS reply packets, so that the address obtained by a user is in the same ISP network with the user. This implementation minimizes web access latency and optimizes user experience.
	DNS Transparent Proxy	Changes the destination addresses of DNS requests and forwards the DNS requests to different ISPs for load balancing.

Category	Function	Description
	PBR	Forwards packets based on applications, services, users, inbound interfaces, source security zones, source IP addresses, destination IP addresses, and time ranges. Supports PBR with a single outbound interface or multiple outbound interfaces. For PBR with multiple outbound interfaces, intelligent uplink selection can be performed based on link bandwidths, weights, qualities, or priorities.
	Global route selection policies	Supports intelligent uplink selection based on equal-cost routes and supports route selection based on link bandwidths, weights, qualities, or priorities.
	ISP link selection	Supports the selection of an outbound interface based on the carrier network of the destination address.
	Health check	Supports service and link availability detection based on multiple protocols.
Routing, Switching, and Packet Forwarding	Switching protocols	Supports common data-link layer protocols including ARP, VLAN protocol and PPP.
	Routing protocols	Supports static routing, routing policies, policy-based routing, RIP, IS-IS, OSPF, BGP, and multicast.
	IP forwarding	Supports basic IP protocols including DNS, DHCP, ICMP, and URPF.
IPv6	Basic IPv6 technologies	Supports the resolution and forwarding of IPv6 packets, the static routing, routing policies, and PBR of IPv6, and the IPv6 dynamic routing protocols such as RIPng, OSPFv3, BGP4+, and IS-ISv6.
	IPv6 transition technologies	Supports IPv6 transition technologies such as 4to6, 6to4, and NAT64, constructs complete IPv6 networks, and functions as the border device of IPv4 and IPv6 networks.
	IPv6 network security protection	● Supports security policies based on IPv6 addresses to protect IPv6 networks. ● Implements packet filtering and content security inspection on packets based on the IPv6 addresses, with the functions and defense effect similar to those of IPv4.
VPN	IPSec/IKE	● Supports IKEv1 and IKEv2. ● Supports encryption algorithms such as DES, 3DES, and AES, and checksum algorithms such as MD5 and SHA1 to provide powerful packet encryption and verification capabilities. ● Supports L2TP over IPSec and GRE over IPSec.

Category	Function	Description
	L2TP	Functions as the LNS.
	GRE	Supports the across-network RIP, OSPF, and BGP over GRE.
	SSL VPN	Supports web proxy, network extension, port forwarding, and file sharing.
	MPLS	● Supports MPLS L3VPN. ● Supports L2TP, IPSec, and GRE access to MPLS VPN. ● Supports IPSec VPN over MPLS.
High Availability	Dual-system hot backup	● Supports dual-system hot backup protocols such as VRRP, VGMP, and HRP. ● Provides a complete dual-system hot backup mechanism to ensure that services are smoothly switched to the standby device when the active device is faulty.
	Cluster	Supports of clustering multiple FWs of different data centers to ensure that the work of a faulty FW can be smoothly taken over by the FWs of other data centers for service continuity in a scenario with multiple active data centers.
	SPU Backup	Supports SPUs working in active/standby backup and load balancing modes. This enables services of a faulty SPU to be smoothly switched to a normal one for service continuity.
	Lossless SPU Scaling	Supports of lossless SPU scaling, which prevents key services from being interrupted during SPU scaling through proper configurations.
	Link status check	Checks the link connection status in real time by sending ARP or ICMP packets or by using BFD and switches traffic when the link is faulty.
Virtual System	Function virtualization	Virtualizes major functions except the hardware and network resources that must be managed in a centralized manner. Each virtual system has its configurations, entries, and resources.
	Virtual administrator	Supports the creation of virtual administrators. Each administrator can be assigned permission to manage the specified virtual system. Each administrator has an independent configuration page for maintaining the device. Virtual systems are isolated, and their configuration does not conflict.

Category	Function	Description
Visualized Management and Maintenance	New Web UI	Provides a new Web UI that offers diversified, easy-to-use, and virtualized management and maintenance functions. On the Web UI, you can easily view logs and reports, manage configurations, and diagnose faults.
	Remote management modes	Supports multiple management modes such as Web UI, CLI (Console, Telnet, or SSH), and NMS (SNMP).
	Update center	On the Web UI, you can update the system software, application signature database, threat signature database, antivirus signature database, and URL category database in various modes to enhance defense capabilities.
	Remote management	You can log in to the device through the console, Telnet, SSH, or in Web mode for management. ● Supports SNMP. You can use standard NMS software for management. ● Supports syslogs. You can use the log server to collect and manage logs. ● Supports NQA and Netstream.
Log and Report	Log	Supports multiple types of logs, such as traffic logs, system logs, and service logs, for the administrator to learn about network events.
	Report	Supports the traffic report for the administrator to gain visibility into the network traffic status.

4.2 Advanced Content Security Defense

The biggest advantage of the next generation firewall is the sophisticated application security capability built on deep application and content inspection.

4.2.1 Accurate Access Control

Conventional security policies use 5-tuple-based packet-filtering rules to control traffic forwarding between security zones. 5-tuple refers to the source address, destination address, source port, destination port, and protocol. The development of Internet technologies brings new requirements for network security and provides more accurate control policies for traffic access. **Table 4-2** lists comparison between conventional and new-generation networks.

Table 4-2 Comparison between conventional and new-generation networks

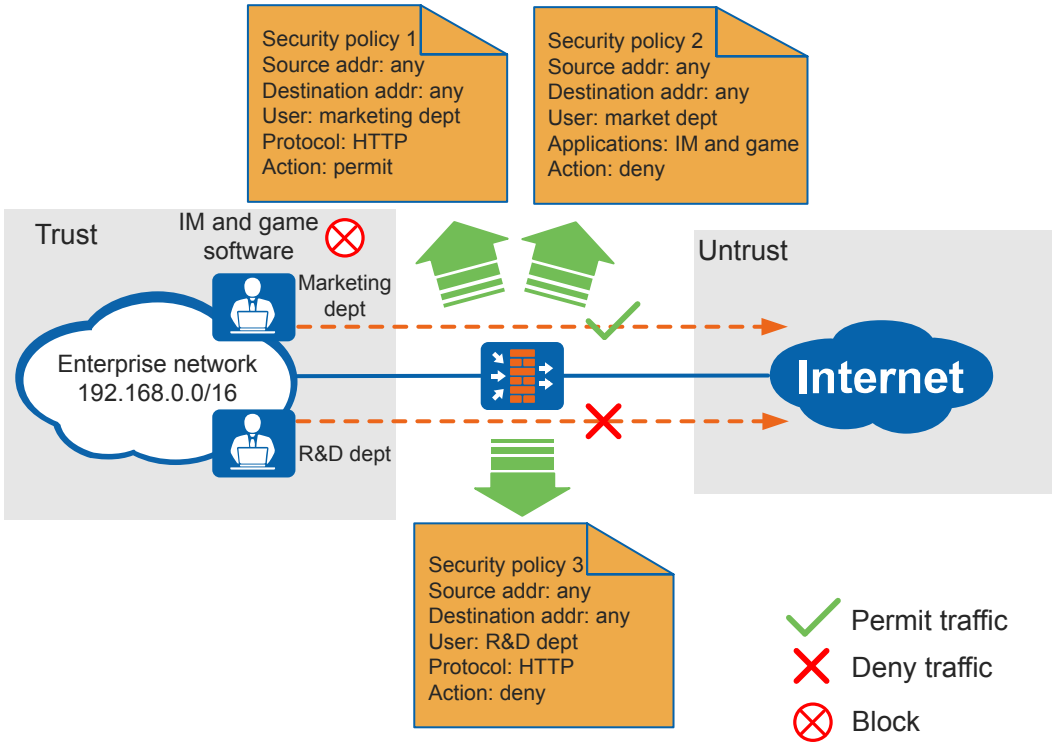
Feature of the Conventional Network	Feature of the New-Generation Network
IP addresses are used to identify users. For example, 192.168.1.0/24 indicates the marketing department. Network segments or security zones are divided to distinguish between users. Users cannot be associated with dynamically obtained IP addresses.	However, enterprise managers hope that users and IP addresses can be dynamically associated; users activities can be queried in a visualized manner; network-traversing applications and contents can be audited and controlled based on user information.
Ports are used to identify applications. For example, web browsing applications use port 80, and FTP uses port 21. To permit or block an application, enable or disable the port used by this application.	However, many applications share the same ports, such as ports 80 and 443. For example, web QQ and web mail both use port 80. Therefore, enabling port 80 permits not only the browsing of Internet pages but also other undesired web-based applications.

On new-generation networks, firewalls are required to identify users and applications to accurately and visually control traffic.

Security policies provided by the FW can not only replace conventional ones and implement user- and application-based traffic control.

As shown in **Figure 4-1**, security policy 1 allows the marketing department to browse Internet pages; security policy 2 prevents the marketing department from using IM or game applications; security policy 3 prevents the R&D department from browsing Internet pages.

Figure 4-1 Security policies configured on the FW



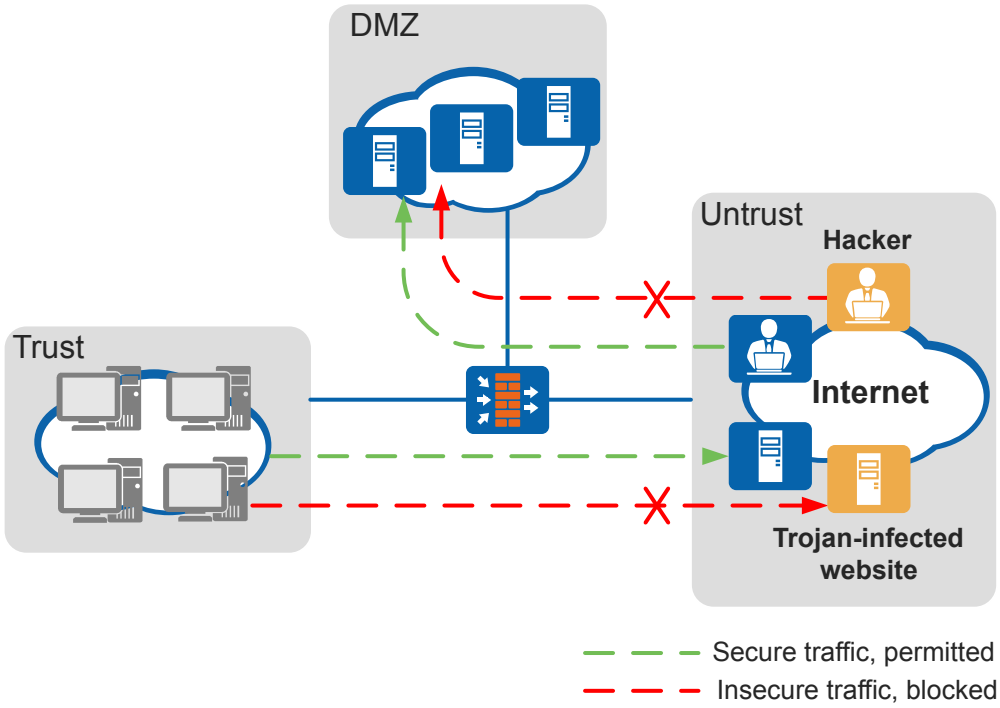
Compared with conventional security policies, the security policies provided by the FW have the following advantages:

- Distinguish between employees from different departments based on "users", making network management more flexible and visualized.
- Distinguish between applications (such as web IM and web game) using the same protocol (such as HTTP), achieving refined network management.

4.2.2 Powerful Intrusion Prevention

IPS analyzes network traffic to detect intrusions (such as buffer overflow attacks, Trojan horses, worms, and botnets) to protect information systems and networks from these intrusions, as shown in **Figure 4-2**.

Figure 4-2 Intrusion prevention scenario



Through the IPS function, the FW monitors or analyzes system events, detects attacks and application layer intrusions, and takes actions to terminate the attacks in real time. The intrusion prevention capabilities of the FW are as follows:

- Supports protection measures based on traffic types.

  You can define refined security policies to implement protection at different levels based on network environments.
- Supports in-depth inspection on application-layer packets.

  The FW has a constantly updated application signature database. It performs in-depth packet inspection on the traffic flows from thousands of applications for attacks and

intrusions. According to configured application-specific security policies, the FW takes actions to the traffic flows from different applications. In this way, the administrator can flexibly deploy the intrusion prevention function.

- Supports attack detection on IP fragments and out-of-order TCP flows.

  Certain attacks use IP packet fragments and out-of-order TCP packets to evade threat detection. To tackle this problem, the FW reassembles the IP fragments into packets or out-of-order packets back in order before performing threat detection.

- Supports a large-capacity signature database and user-defined signatures.

  IPS-capable devices use signatures to identify attack traffic. The signature database capacity represents the application-layer threat identification capability.

  The predefined signature database of the FW can identify thousands of application layer attacks. The constant update of the signature database keeps the application identification and attack defense capabilities of the FW up-to-date. In addition, administrators can define signatures based on traffic information to enhance the intrusion prevention function of the FW.

4.2.3 Refined Traffic Management

Network services develop rapidly, but network bandwidth is limited. If necessary, you can manage bandwidth resources to ensure enough bandwidth for high-priority services and reduce bandwidth resources used by low-priority services.

You may encounter the following problems during network bandwidth management:

- P2P traffic consumes most bandwidth.
- Hosts cannot access services provided by enterprises due to DDoS attacks.
- Stable bandwidth or connection resources cannot be guaranteed for specific services.
- Overloading service traffic deteriorates user experience.

The following traffic management technologies of the FW can tackle these problems:

- Allocate bandwidth and connection resources based on IP addresses, users, applications, and time, reducing bandwidth consumed by P2P traffic and granting certain users P2P download permissions.
- Limit the bandwidth for security zones (bandwidth management) or interfaces (QoS) to protect intranet servers and network devices from DDoS attacks.
- Allocate different maximum bandwidths to applications as needed. The powerful application identification capability helps the FW implement refined bandwidth management.

The FW flexibly allocates bandwidth based on traffic policies and traffic profiles. Each traffic profile represents a range of available bandwidth or connection resources. Each traffic policy assigns a traffic profile to a type of traffic. There are two bandwidth allocation methods:

- Traffic policies share one traffic profile. Traffic flows matching the traffic policies preempt bandwidth and connection resources defined in the traffic profile to improve the efficiency of network resources. You can also set the per-IP or per-user maximum bandwidth, preventing network congestion or bandwidth exhaustion by certain hosts.
- One traffic policy exclusively uses one traffic profile. This mode guarantees bandwidth for high-priority services or hosts.

4.2.4 Perfect Load Balancing

Enterprises may deploy multiple links on each network egress or multiple servers to share traffic and improve user experience. How can these links or servers collaborate to share the traffic? Inbound and outbound load balancing provided by the FW can address this issue.

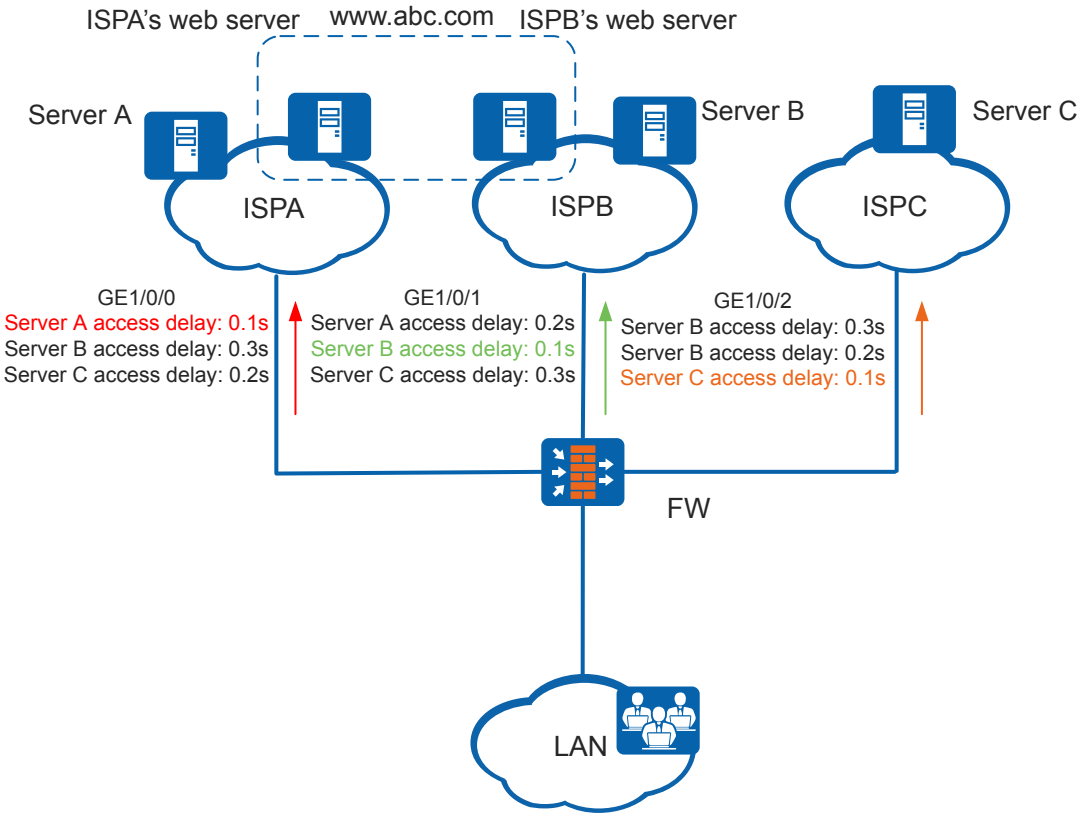
Outbound Load Balancing

When multiple links are deployed on an enterprise network egress, outgoing traffic is evenly distributed among these links usually. This method improves network stability and reliability but may not meet the following requirements:

- Forward traffic destined for an ISP network is through the outgoing interface connected to the ISP network.
- When a service is deployed on multiple ISP networks, evenly distribute traffic from the enterprise network to ISP networks through their respective links to avoid congestion.
- Forward user traffic destined for a server on the Internet through the path with the smallest delay to avoid congestion.

The FW supports outbound load balancing functions, such as ISP link selection, transparent DNS, and intelligent link selection, easily meeting the previous requirements and applying to various multi-link load balancing scenarios.

Figure 4-3 Outbound load balancing



- ISP link selection

  When an enterprise network has links to multiple ISP networks, you can add the network address of each ISP to a specific ISP address file, import the file to the FW, and specify the next hop or outgoing interface for the ISP address file to generate static routes to the ISP networks in batches. User traffic is forwarded to the corresponding ISP network based on a matching static route. This mechanism ensures that traffic destined for a specific ISP network is forwarded through the corresponding outgoing interface, not diverting to other ISP networks.

- Transparent DNS

  After transparent DNS is configured, the FW changes the destination addresses of DNS requests and sends the requests to DNS servers on different ISP networks based on weights (percentage). In this way, the traffic of the intranet is balanced between the ISP links to avoid congestion and improve user experience.

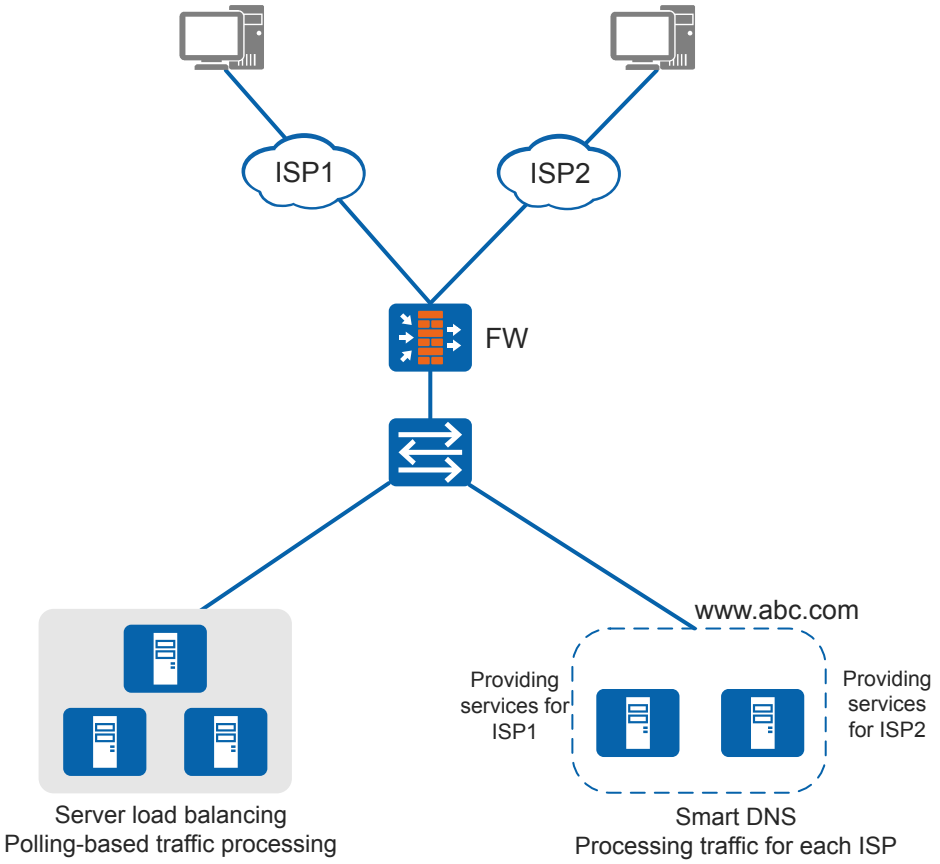
- Intelligent uplink selection

  Intelligent link selection detects the delay of the links to a remote host and selects the optimal link with the shortest delay to forward services rapidly. In addition, you can manually set a route weight and bandwidth threshold for each link based on link performance, so that service traffic can be forwarded through different links as planned.

Inbound Load Balancing

Inbound load balancing properly distributes traffic from external users to internal servers. The FW supports server load balancing and Smart DNS.

Figure 4-4 Inbound load balancing



- Server load balancing

  Service requests are processed by multiple servers to improve efficiency and performance. These real servers form a server cluster, acting as one logical server. For users, there is only one server. The FW allocates traffic to real servers. If one real server fails, the FW no longer allocates traffic to it. If the capacity of the cluster is insufficient, you must add servers to it. The internal changes are transparent to users, facilitating network O&M and future adjustment.

  Server load balancing allows traffic to be evenly distributed to servers. The FW can adjust traffic allocation algorithms based on service types, meeting special service requirements and improving service quality and efficiency. The following algorithms are available:

  - Round robin algorithm

    Sends service requests to servers in turn.
  - Weighted round robin algorithm

    Sends service requests to servers based on weights.
  - Least connection algorithm

    Sends service requests to the server with the least concurrent connections.
  - Weighted least connection algorithm

    Sends service requests to the server with the least weighted concurrent connections.
  - Sticky session algorithm

    Always sends service requests from one user to a fixed server using the source IP address-based hash algorithm.
  - Weighted session sticky session algorithm

    Always sends service requests from one user to a fixed server, and sends more traffic to higher-weighted servers.
- Smart DNS

  When an enterprise network has a DNS server, the FW intelligently sends the IP address of the outgoing interface connected to the ISP network that serves the requesting user to minimize latency and improve user experience.

5 Operation and Maintenance

5.1 Maintenance Features and Functions

5.1.1 System Configuration Mode

The USG9500 provides the following three configuration modes:

- Command line configuration
- Web configuration
- NMS configuration

The command line configuration supports:

- Local configuration through the console port
- Remote configuration through the AUX port with a Modem
- Remote configuration through Telnet or SSH
- Configuration management on web pages

The NMS configuration supports HUAWEI NMS that is based on SNMP.

5.1.2 System Management and Maintenance

The USG9500 provides the following system management and maintenance functions:

- Board-in-position detection, hot-swap detection, board reset, control over running and debugging indicators, fan monitoring, power monitoring, active/standby switchover control, and version query
- Signature databases can be upgraded locally or online. The system software and configuration file can be rolled back, backed up, saved, and deleted.
- Hierarchical user permission management, operation log management, online help and comment for command line
- Simultaneous operation by multiple administrators
- Hierarchical management, alarm classification, and alarm filtering

5.1.3 System Service and Status Tracking

The USG9500 tracks the system service and status, including:

- Monitor the migration of state machines related to routing protocols
- Monitor the migration of state machines related to VPN
- Monitor the types of protocol packets that are sent by the NP and display details on the packets with the debugging function
- Monitor and count abnormal packets
- Monitor and collect statistics on the resources that are occupied by each system feature

5.1.4 System Test and Diagnosis

The USG9500 provides service debugging functions. It records online the information about key events, packet processing, packet resolution, and state switchover during the specified time. You can enable or disable debugging functions on the console based on the specified service (such as a certain routing protocol) and specified interface (such as an interface on which a routing protocol runs).

The CPU usage of the MPU, SPU, and LPU can be queried in real time.

The debugging and trace messages are classified into different levels. According to the configuration, these messages with different levels can be redirected to various output destinations, such as the console, syslog server, and SNMP trap trigger alarm.

5.1.5 Online Upgrade

The USG9500 supports online software upgrade. If the upgraded software is faulty, you can restart the system and roll back to the original software version. Meanwhile, the USG9500 supports online software patching, that is, you only need to upgrade certain necessary features. If the patched software is faulty, you can roll back to the original software version.

Board program upgrade downloads programs online. During the upgrade, you need to reset only the board to be upgraded. For upgrading LPU programs, you can upgrade multiple concurrent LUP programs at the same time. After that, original programs are backed up on the device. Online program downloading does not affect the normal running of the system.

5.1.6 Other Features

The USG9500 provides the following additional features:

- Hierarchical commands, ensuring that unauthorized users cannot access the device
- Online help available if you type a question mark (?)
- Various debugging information for troubleshooting
- Command execution history
- Fuzzy search for command lines, for example, you can enter the non-conflicting key words "**disp**" for the **display** command

5.2 Network Management

The USG9500 uses the VSM system for network management. This network management system supports SNMP(V1/V2c/V3) and the client/server architecture and can run on multiple operating systems independently. The supported operating systems include Windows NT/2000 and UNIX (SUN, HP, and IBM).

5.3 WEB Configuration and Management

USG9500 provides a web graphic user interface (GUI) for user-friendly configuration and management. On the GUI, you can configure features, such as security zones, ACLs, NAT, ASPF, attack defense, blacklists, and IPS and view various statistics parameters.

The web browser communicates with the USG9500 over the HTTP Secure (HTTPS) protocol. HTTPS employs the SSL security encryption mechanism to establish an encrypted channel between the client and server, preventing data from being eavesdropped. The encryption function ensures the security of user information.

5.4 Security

Data System Security

The system uses data backup and recovery to ensure data security. Save the data (including the system software, configuration file, log file, and database data) at a certain timepoint to another storage device. When anomalies occur in the system, you can import the backup data to the system to restore the system.

Operation and Maintenance Security

The USG9500 provides a security mechanism to ensure the security of operation and maintenance from multiple dimensions, such as device management, application, and log.

- Hierarchical administrator management

  The USG9500 supports hierarchical management of administrators. Administrators have different permissions. They must enter the correct user name and password to log in to the system. After they successfully log in to the system, they can perform only the authorized operations.

- Access channel control

  The USG9500 provides a dedicated out-of-band management port instead of using the service ports for management.

  The device uses the ACL and policy mechanism to ensure the security of device access.

  The USG9500 uses security protocols to communicate with third-party NMSs. You can enable security protocol services, such as HTTPS, and disable the services of insecure protocols, such as Telnet.

- Logging

  The USG9500 logs important operations, such as login and logout, for future audit.

- Protection of sensitive user information

  The USG9500 authenticates users through password authentication and protects sensitive user information using the advanced encryption algorithm. Each user is allocated with a default password. The USG9500 checks the validity of their passwords when they access the USG9500. When administrators log in to the USG9500, the USG9500 forces them to change the default password to enhance security.

- Anti-brute-force

  To prevent unauthorized users from hacking into the system by conjecturing the administrator's user name and password, the USG9500 sets a maximum number of login attempts. Once the number of login attempts exceeds the specified threshold, the system adds the user's IP address to the isolated IP address list and blocks the user from accessing the device within the lockout period.

- Management plane isolation

  The USG9500 supports the isolation of the in-band management plane. You can configure corresponding security policies to ensure the security of the management plane.

  If users connect to the USG9500 from the service interface and use a management protocol, such as Telnet, SSH, or HTTPS, to log in to the device, you can configure the policy for the interzone between the Local zone and the security zone to which the service interface is added to prohibit the users from managing the device. In this way, the security isolation is implemented.

Device Access Security

The USG9500 provides a security protection mechanism for the console port, service port, and management port GigabitEthernet 0/0/0. You can configure functions, such as security policies, port lockup, and blacklist, to avoid brute force and prevent unauthorized login.

6 Technical Specifications

6.1 Standards and Protocols

Table 6-1 Standards and protocols

Standard	Content
ETS 300 386	Electromagnetic compatibility and Radio spectrum Matters (ERM); Telecommunication network equipment; Electromagnetic Compatibility (EMC) requirements
IEC 62151	Safety of equipment electrically connected to a telecommunication network
IEEE 802.1d	MAC bridges
IEEE 802.1p	Traffic Class Expediting and Dynamic Multicast Filtering
IEEE 802.1q	Virtual Bridged Local Area Networks
IEEE 802.3u	Definition of Fast Ethernet (100BTX, 100BT4, 100BFX)
IEEE 802.3z	Definition of Gigabit Ethernet (over fiber)
ITU-T G.652	Characteristics of a single-mode optical fiber and cable
RFC0768	User datagram protocol (UDP)
RFC0791	Internet protocol (IP)
RFC0792	Internet Control Massage Protocol (ICMP)
RFC0793	Transport Control Protocol (TCP)
RFC0854	Telnet
RFC0894	Technical specification For network access server
RFC1157	Simple Network Management Protocol (SNMP)

Standard	Content
RFC1213	Management information base for network management of TCP/IP-based Internets: MIB-II
RFC1229	Extensions to the generic-interface MIB
RFC1661	Point-to-point links (PPP)
RFC1757	Remote network monitoring management information base
RFC2865	Remote authentication dial-in user service (RADIUS)
RFC2869	RADIUS extensions
RFC2903	Generic AAA architecture
RFC2904	AAA authorization framework
RFC2906	AAA authorization requirements
RFC2809	Implementation of L2TP compulsory tunneling via RADIUS
RFC1492	An access control protocol, sometimes called TACACS
RFC2401	Security architecture for the Internet protocol
RFC2402	Authentication header (AH)
RFC2403	The Use of HMAC-MD5-96 within ESP and AH
RFC2404	The Use of HMAC-SHA-1-96 within ESP and AH
RFC2405	The ESP DES-CBC cipher algorithm with explicit IV
RFC2406	IP encapsulating security payload (ESP)
RFC2407	The Internet IP security domain of interpretation for ISAKMP
RFC2408	Internet security association and key management protocol (ISAKMP)
RFC2409	Internet key exchange (IKE)
RFC2410	The NULL encryption algorithm and its use with IPSec
RFC3715	IPSec-Network Address Translation (NAT) Compatibility Requirements
RFC3947	Negotiation of NAT-Traversal in the IKE
RFC2663	IP Network Address Translator (NAT) Terminology and Considerations
RFC 2578	Structure of management information version 2 (SMIv2)
RFC 2579	Textual conventions for SMIv2
RFC2580	Conformance statements for SMIv2
RFC1157	SNMP

Standard	Content
RFC1155	Structure and identification of management information for TCP/IP-based Internets
RFC1213	Management information base for network management of TCP/IP-based Internets: MIB-II
RFC1212	Concise MIB definitions
RFC1901	Introduction to community-based SNMPv2
RFC1035	NTPv3 specification
RFC854	Telnet protocol specification
RFC857	Telnet echo option
RFC858	Telnet "Suppress Go Ahead" option
RFC1091	Telnet terminal type option
RFC4250	The Secure Shell (SSH) Protocol Assigned Numbers
RFC4251	The Secure Shell (SSH) Protocol Architecture
RFC4252	The Secure Shell (SSH) Authentication Protocol
RFC4253	The Secure Shell (SSH) Transport Layer Protocol
RFC4254	The Secure Shell (SSH) Connection Protocol
RFC4255	Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints
RFC4256	Generic Message Exchange Authentication for the Secure Shell Protocol (SSH)
RFC4335	The Secure Shell (SSH) Session Channel Break Extension
RFC4344	The Secure Shell (SSH) Transport Layer Encryption Modes
RFC4419	Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol
RFC4462	Generic Security Service Application Program Interface (GSS-API) Authentication and Key Exchange for the Secure Shell (SSH) Protocol
RFC1350	TFTPv2
RFC959	FTP
RFC1945	Hypertext Transfer Protocol -- HTTP/1.0
RFC2145	Use and Interpretation of HTTP Version Numbers
RFC2616	Hypertext Transfer Protocol -- HTTP/1.1
RFC2617	HTTP Authentication: Basic and Digest Access Authentication

Standard	Content
RFC2774	An HTTP Extension Framework
RFC2965	HTTP State Management Mechanism
RFC2787	Definitions of managed objects for the virtual router redundancy protocol
RFC1828	IP Authentication using Keyed MD5
RFC1829	The ESP DES-CBC Transform
RFC1851	The ESP Triple DES Transform
RFC2085	HMAC-MD5 IP Authentication with Replay Prevention
RFC2104	HMAC: Keyed-Hashing for Message Authentication
RFC2402	IP Authentication Header
RFC2403	The Use of HMAC-MD5-96 within ESP and AH
RFC2404	The Use of HMAC-SHA-1-96 within ESP and AH
RFC2406	IP Encapsulating Security Payload (ESP)
RFC2407	The Internet IP Security Domain of Interpretation for ISAKMP
RFC2408	Internet Security Association and Key Management Protocol (ISAKMP)
RFC2409	The Internet Key Exchange (IKE)
RFC2451	The ESP CBC-Mode Cipher Algorithms
RFC2792	DSA and RSA Key and Signature Encoding for the KeyNote Trust Management System
RFC3447	Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1
RFC3602	The AES-CBC Cipher Algorithm and Its Use with IPsec
RFC3947	Negotiation of NAT-Traversal in the IKE
RFC4109	Algorithms for Internet Key Exchange version 1 (IKEv1)
RFC4301	Security Architecture for the Internet Protocol
RFC4302	IP Authentication Header
RFC4303	IP Encapsulating Security Payload (ESP)
RFC4306	Internet Key Exchange (IKEv2) Protocol
VGMP	VRRP Group Management Protocol
HRP	Huawei Redundancy Protocol