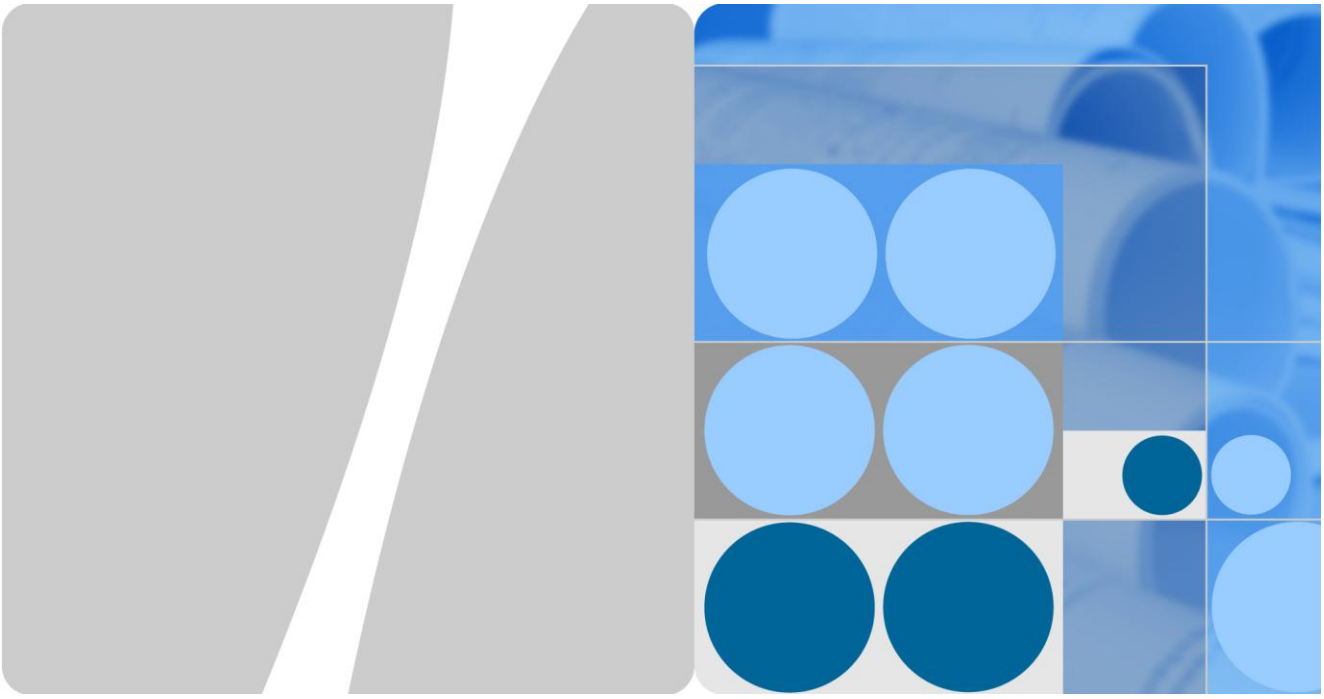


Secospace USG2000/5000 Unified Security Gateway V300R001

Product Description

Issue 03

Date 2013-05-08

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://enterprise.huawei.com

About This Document

Product Version

The following table lists the product versions of this document.

Product Name	Product Version
Secospace USG2110-X/2100/2200/5100/5500	V300R001

Unless otherwise specified, all the previous products are referred to as the USG in this document.

Intended Audience

This document describes the product positioning, functions and features, software and hardware architecture, service features and application scenarios, standard compliance, and technical specifications of the Secospace USG.

It provides an overview the USG.

This document is intended for:

- Network planning engineers
- Data configuration engineers
- System maintenance engineers
- Network administrators

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
	Indicates a hazard with a high level or medium level of risk which, if not avoided, could result in death or serious injury.

Symbol	Description
 WARNING	Indicates a hazard with a low level of risk which, if not avoided, could result in minor or moderate injury.
 CAUTION	Indicates a potentially hazardous situation that, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results.
 TIP	Provides a tip that may help you solve a problem or save time.
 NOTE	Provides additional information to emphasize or supplement important points in the main text.

Update History

Updates between document issues are cumulative. Therefore, the latest document issue contains all updates made in previous issues.

Updates in Issue 03 (2013-05-08)

The third official release.

Updates in Issue 02 (2013-01-25)

Second official release. Added the location identifier of ESN in the panel in the appearance description of 3.1 Hardware Structure.

Updates in Issue 01 (2012-11-06)

First official release.

Contents

1 Product Orientation

USG5500 Series

The USG5500 series is a new-generation carrier-class Unified Security Gateway developed by Huawei Technologies Co., Ltd. (Huawei) for large and medium-sized enterprises and carriers. The USG5500 series can be deployed at the network edges of carriers, government agencies, and organizations in industries such as finance, energy, and education.

The USG5500 series comes in 1-U and 3-U models. It provides multiple fixed Gigabit Ethernet ports and expansion slots to hold a wide range of extra interface cards such as 10GE ports.

This series uses the new 10-Gigabit multi-core hardware platform to constructs a high-speed network with no delay for processing mass services; by integrating advanced intrusion prevention and anti-virus technologies, it delivers content security protection and builds a securer network; with the industry-leading deep packet inspection (DPI) technology, it manages thousands of application programs subtly and provides a more effective network. The USG5500 series helps data centers and large and medium-sized enterprises to build a cost-effective network with higher speed, efficiency, and security. The USG5500 series can be deployed at borders of carriers, enterprises, governments, financial institutes, energy companies, and campus networks.

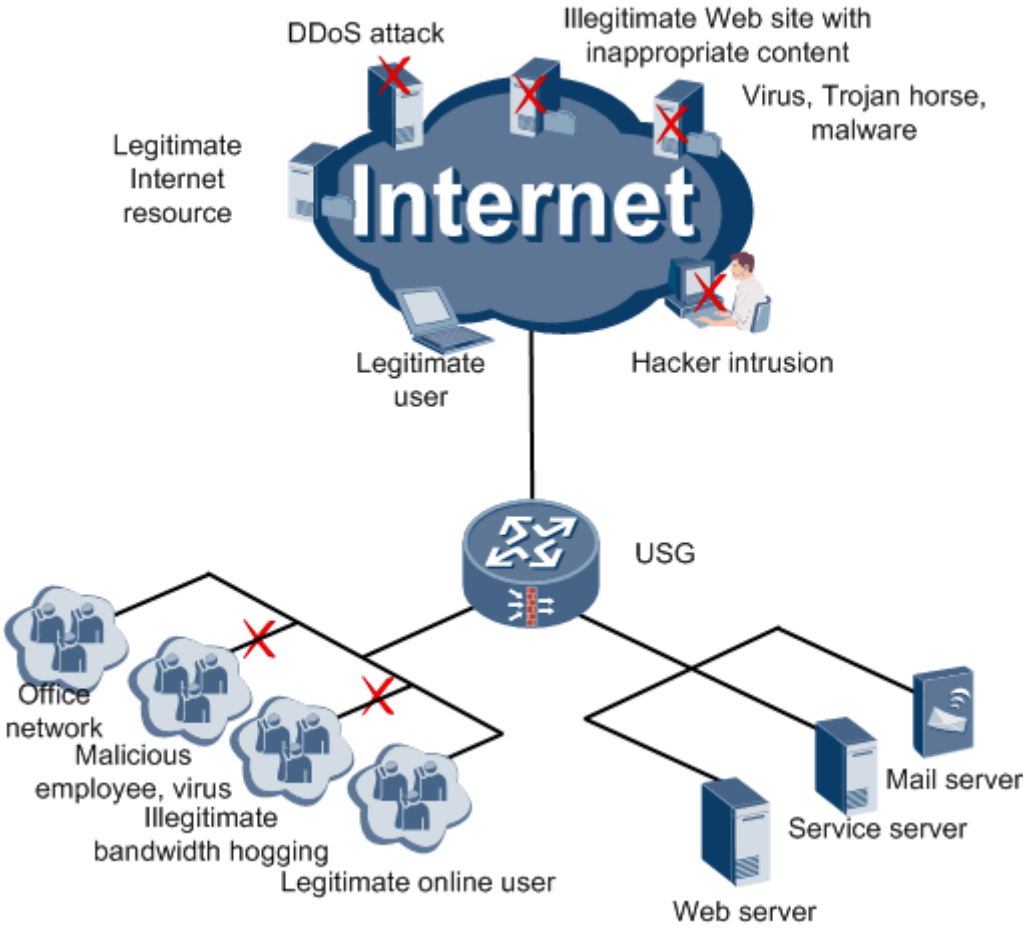
Besides basic firewall functions, the USG5500 series also supports a wide variety of routing protocols, saving investments and deployment costs.

The USG5500 series supports IPv4 and IPv6 dual stacks and complete IPv6 features, enabling a smooth IPv4-to-IPv6 transition.

With the Unified Threat Management (UTM) functions, the USG5500 series can provide content security and online behavior management, offering all-around security protection.

As shown in Figure 1-1, the USG5500 is deployed at the network egress to prevent hacker intrusions and DDoS attacks from the Internet, block illegitimate Web sites for intranet users, and control bandwidth usage to maintain a secure and reliable intranet.

Figure 1-1 USG5500 series application



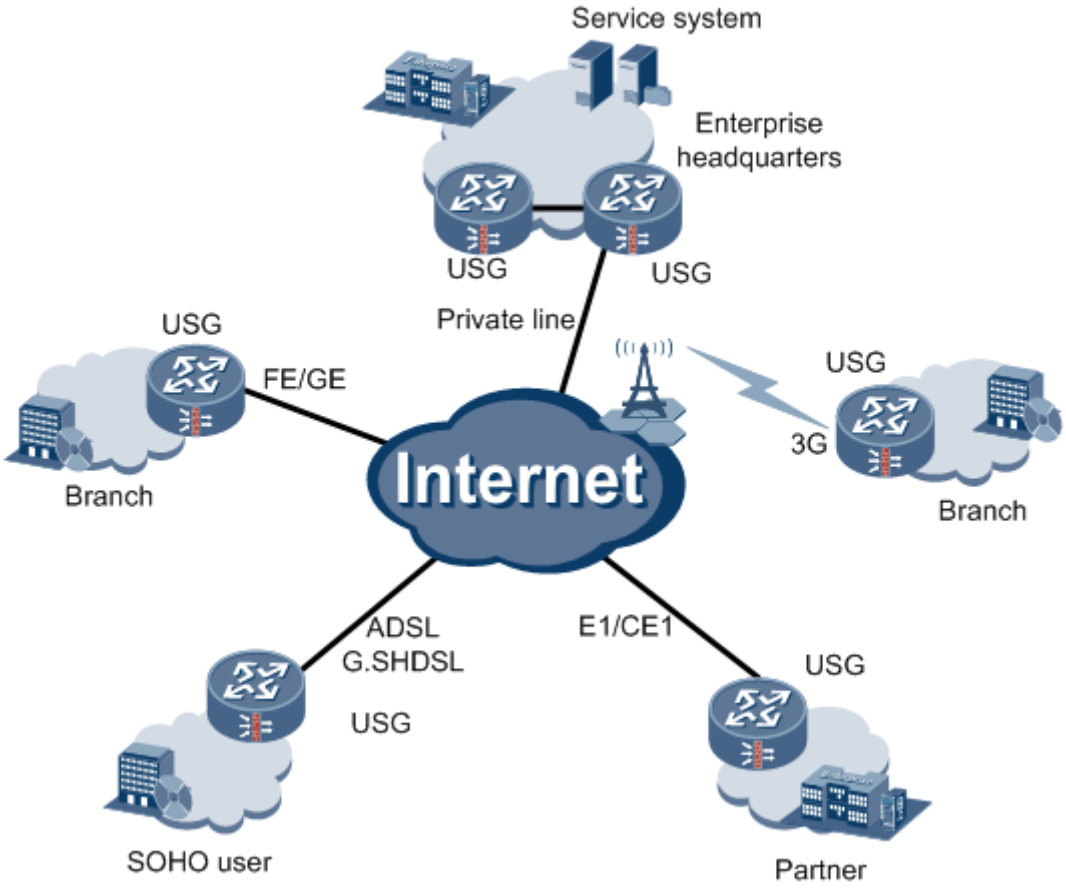
USG2110-X/2100/2200/5100 Series

The USG2110-X/2100/2200/5100 series is a new-generation product launched by Huawei to meet the requirements of small and medium-sized enterprises, branches of large enterprises, SOHO users, and cyber bars.Figure 1-2 shows the application of the USG2110-X/2100/2200/5100 series.

Based on the modular design, the USG2110-X/2100/2200/5100 series integrates multiple features such as security, routing, switching, and wireless (WiFi and 3G) features. With varieties of interface types and industry-leading performance, the USG2110-X/2100/2200/5100 series delivers sound security protection for small and medium-sized enterprises, branches of large enterprises, SOHO users, and cyber bars. In addition, the USG2110-X/2100/2200/5100 series provides the integrated network egress security and interworking solution, which helps enterprises decrease cost and increase production efficiency. The USG2110-X/2100/2200/5100 series, as a security protection device, is an ideal option for small and medium-sized enterprise networks.

The USG2110-X/2100/2200/5100 series integrates multiple services, and is excellent in terms of the reliability, processing capability, modular port, and service capability, which greatly reduces the initial investment and long-term operation and maintenance costs of the construction of enterprise networks.

Figure 1-2 USG2110-X/2100/2200/5100 series application



2 Product Features

The USG5500 Applies the New 10-Gigabit Multi-Core Hardware Platform and Constructs A High-Speed Network for Users

- Provides prominent performance, delivering mass service processing capability.
- Provides high-density 10-Gigabit interfaces, to accommodate different scenarios for 10G customers so that they can add ports to different zones.
- Provides key components redundancy, mature link switchover mechanism, and built-in bypass cards for both optical and electrical links, preventing hardware faults for a long period and making a sustainable working environment for users.

Integrated Service

- Integrates security, routing, switching, VPN, and wireless functions, which greatly enhances the product integration capability.
- Completely integrates the functions of the Ethernet switch.
- Provides the Wireless Local Area Network (WLAN) function and Internet access through the Ethernet, ADSL2+, SHDSL, E1/CE1, serial, and 3G on the USG2110-X/2100/2200/5100.
- Provides users with all the router, firewall, switch, VPN, and wireless features on a single device.

Refined Management over Thousands of Application Programs, Building an Efficient Network

- Identifies wide ranges of application layer protocols, providing visibility into the applications running on the network.
- Equips with mass Web sites, blocking Trojan horse-embedded and phishing Web sites, isolating pornographic and gambling Web sites, and preventing employees against maloperations.
- Offers multi-dimensional control measures specific to time, application, user, bandwidth, and connection number, effectively providing bandwidths for mission-critical applications, improving bandwidth usage and working efficiency.

Professional Content Security Defense, Providing a Secure Network

- Provide 99% detection ratio by using the AV engine that is built on the anti-virus technologies and has file-level scanning capability, and the world-leading emulation environment and virtual execution technology.
- Provides professional vulnerability patching technology to prevent attack variants: In the traditional attack code-based defense mode, a huge signature database needs to be maintained and updated due to the transformation of attack types, which overloads the IPS engine and leads to low detection performance and high false negative and false positive ratios. The USG is backed by advanced vulnerability defense technology and delivers virtual patches for vulnerabilities (not attack code), preventing attack variants.
- Maintains a professional team to provide updates, tracking the latest, most widespread, and most dangerous system and software vulnerabilities, and defending against attacks quickly, to improve the security of office networks.

One-Key Configuration, Freeing Users from Complicated Policy Optimization

- Provides a Web interface to make device management and configuration simple and intuitive.
- Provides wizards for key configurations, guiding administrators through the configuration processes.
- Provides one-key enabling of IPS and AV, freeing the administrators from repeated, strenuous, and time-consuming policy configuration efforts and make the device plug-and-play.

Identification-based Intranet Control and Policy Unification

- Provides multiple user authentication mechanisms: local user database authentication, portal authentication, and transparent authentication based on the data imported from the connected third-party servers as RSA secureID.
- Delivers unified security policies, providing refined traffic control by users or user groups, application protocols categories, time periods, IP segments, and ports based on the accurate identification of users or user groups and application protocol categories; Completes the configurations such as packet filtering, UTM, and application detection and control at one time.

Flexible Scalability

Uses the independently developed software platform and Huawei-proprietary security operating system, separating the data plane and the management plane, which enhances the system security; provides brilliant flexibility and configurability with open Application Programming Interfaces (APIs), for further development and evolution.

Supports multiple new storage media such as the USB disks, CF cards, and microSD cards, providing high scalability.

Provides FE ports, GE ports, console ports, microSD card slots, and optional DMIC, FIC, and DFIC expansion slots; uses a modular design, improving scalability, facilitating future upgrade and maximizing investment protection.

3 Product Architecture

About This Chapter

3.1 Hardware Structure

3.1.1 Product Appearance of the USG2110-X Series

Product Model

The USG2110-X series has the following models::

- USG2110-F (two WAN Ethernet interfaces; eight switching LAN Ethernet interfaces)
- USG2110-F-W (two WAN Ethernet interfaces; eight switching LAN Ethernet interfaces; the WLAN function is supported)
- USG2110-A-W (one WAN Ethernet interface; eight switching LAN Ethernet interfaces; one ADSL interface; the WLAN function is supported)
- USG2110-A-GW-W (one WAN Ethernet interface; eight switching LAN Ethernet interfaces; one ADSL interface; the WLAN and WCDMA 3G functions are supported)
- USG2110-A-GW-C (one WAN Ethernet interface; eight switching LAN Ethernet interfaces; one ADSL interface; the WLAN and CDMA2000 3G functions are supported)

For the model with the 3G function, the 3G data card is already installed and thus no additional 3G data card is required; For other models, external USB 3G data cards are required to implement the 3G function.

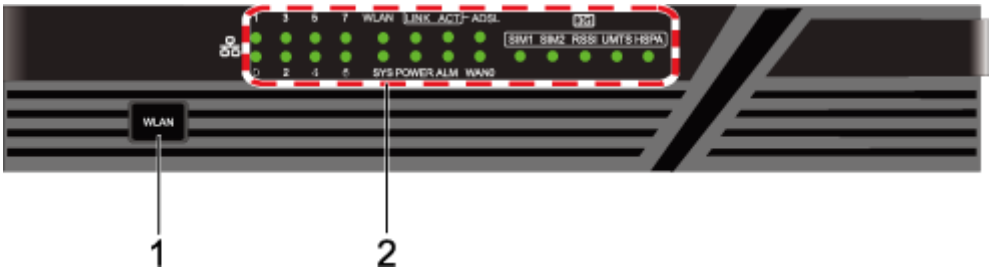
Product Appearance

NOTE

Please refer color and shape to product. Reserves the right to make changes or improvements to any of the products without prior notice.

The following figures takes the USG2110-A-GW-W as an example.

Figure 3-1 Front Panel

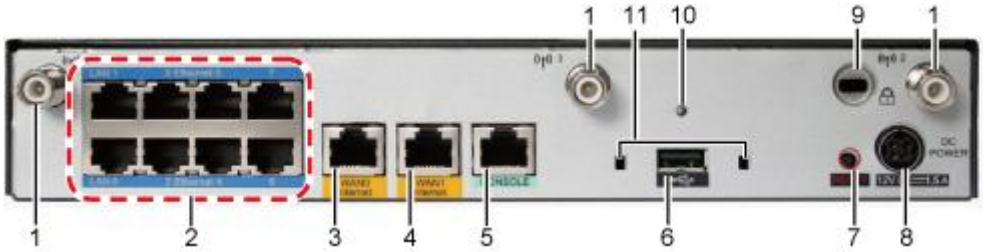


1. WiFi on-off
2. Indicator

Figure 3-2 Rear Panel of USG2110-F

1. 10/100M LAN interface
2. WAN0 interface
3. WAN1 interface
4. Console port
5. USB2.0 interface
6. Reset button
7. Power socket
8. Security lock hole
9. USB anti-theft installation hole
10. USB anti-theft locating hole

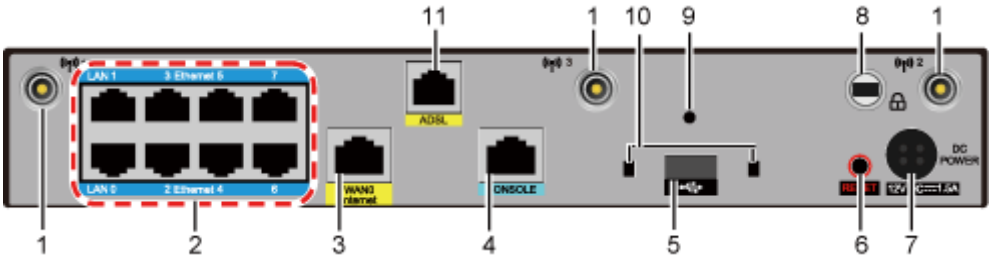
Figure 3-3 Rear Panel of USG2110-F-W



1. WiFi antenna connectors	2. 10/100M LAN interface
3. WAN0 interface	4. WAN1 interface
5. Console port	6. USB2.0 interface
7. Reset button	8. Power socket

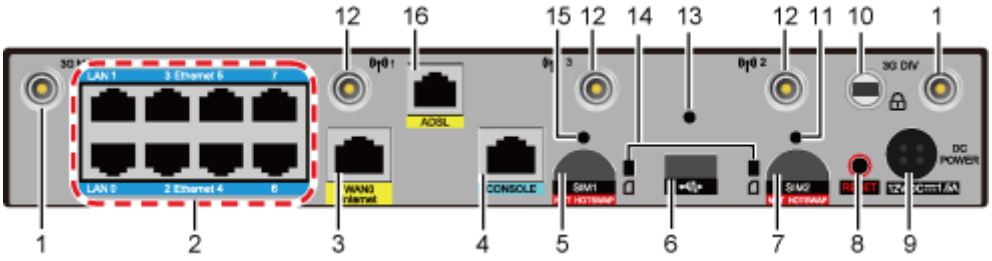
9. Security lock hole	10. USB anti-theft installation hole
11. USB anti-theft locating hole	-

Figure 3-4 Rear Panel of USG2110-A-W



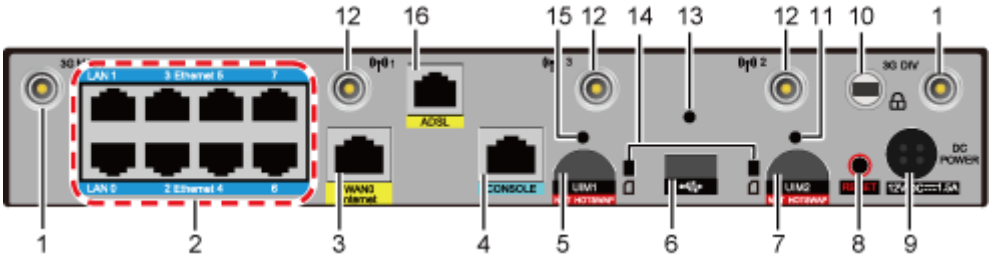
1. WiFi antenna connectors	2. 10/100M LAN interface	3. WAN0 interface
4. Console port	5. USB2.0 interface	6. Reset button
7. Power supply	8. Security lock hole	9. USB anti-theft installation hole
10. USB anti-theft locating hole	11. ADSL interface	

Figure 3-5 Rear Panel of USG2110-A-GW-W



1. 3G antenna connectors	2. 10/100M LAN interface	3. WAN0 interface
4. Console port	5. SIM1 slot	6. USB2.0 interface
7. SIM2 slot	8. Reset button	9. Power supply
10.Security lock hole	11.SIM2 anti-theft installation hole	12.WiFi antenna connectors
13.USB anti-theft installation hole	14.USB anti-theft locating hole	15.SIM1 anti-theft installation hole
16.ADSL interface		

Figure 3-6 Rear Panel of USG2110-A-GW-C



1. 3G antenna connectors	2. 10/100M LAN interface	3. WAN0 interface
4. Console port	5. UIM1 slot	6. USB2.0 interface
7. UIM2 slot	8. Reset button	9. Power supply
10.Security lock hole	11.UIM2 anti-theft installation hole	12.WiFi antenna connectors
13.USB anti-theft installation hole	14.USB anti-theft locating hole	15.UIM1 anti-theft installation hole
16.ADSL interface		

3.1.2 Product Appearance of the USG2100 Series

The USG2100 series include the following models, which are all 1U devices:

- USG2160 (two MIC slots, without WiFi)
- USG2160W (two MIC slots, with WiFi)

Front Panel

The front panel of the USG2100 series are similar. The following takes the USG2160W for example.

Figure 3-7 Front panel of the USG2160W

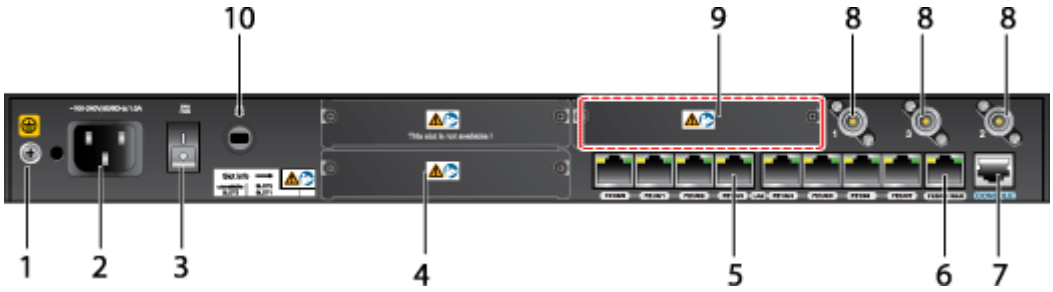
1. ESN	2. USB2.0 interface	3. WiFi switch
4. Flash memory interface	5. Indicator	6. Reset button

NOTE

USG2160 do not support the WiFi function. The WiFi switch and indicator are not provided on the front panel.

Rear Panel

Figure 3-8 Rear panel of the USG2160W



1. Grounding terminal	2. AC power supply socket	3. AC power switch
4. MIC1/DMIC1 slot(SLOT2)	5. LAN interface(SLOT1)	6. WAN interface(SLOT0)
7. Console port	8. WiFi antenna connector	9. MIC2 slot(SLOT3)
10. Security lockhole		

Figure 3-9 Rear panel of the USG2160

NOTE

The USG2160 does not support the WiFi function. The WiFi antenna connector is not provided on the rear panel.

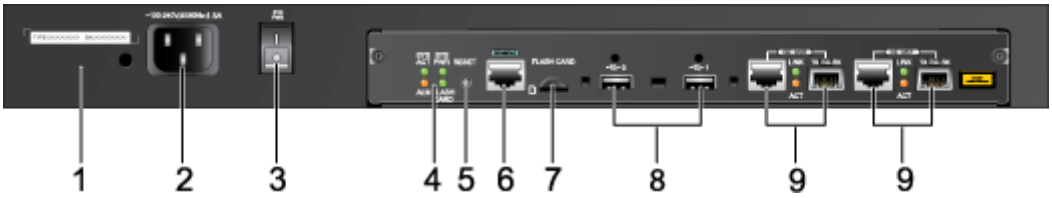
3.1.3 Product Appearance of the USG2200 Series

Front Panel

The USG2200 series includes USG2230 and USG2260, all of which have AC models. Each device consists of an integrated chassis and expansion interface cards. Each device is of 1 U height and provides four MIC slots and two FIC slots. The power supply and fan modules are not hot-swappable and fixed in the USG2200 series.

Figure 3-10 shows the front panel of the USG2200.

Figure 3-10 Front panel of the USG2200 Series

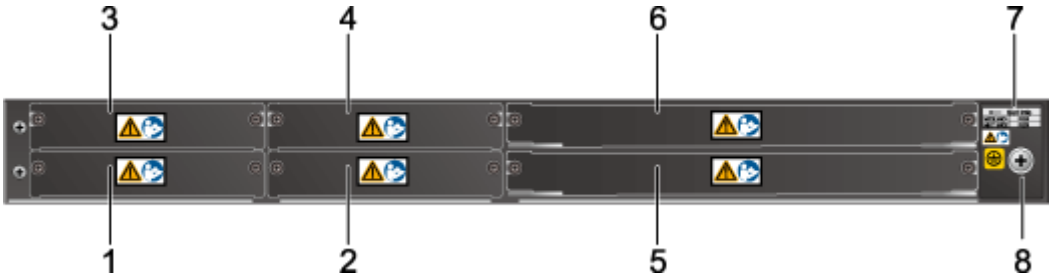


1. ESN
2. Power socket
3. Power switch
4. Indicator
5. Reset button
6. Console port
7. microSD card slot
8. USB port
9. GE combo port

Rear Panel

Figure 3-11 shows the rear panel of the USG2200.

Figure 3-11 Rear panel of the USG2200 Series



1. MIC1/DMIC1
2. MIC2/DMIC2
3. MIC3
4. MIC4
5. FIC5/DFIC5
6. FIC6
7. Slot identifier
8. Grounding terminal

The USG2230/2260 includes the minimum configuration and the AC model basic configuration. The minimum configuration provides no expansion card slot, and the AC model basic configuration provides two 1GE interface cards. Figure 3-12 shows the rear panel of the device.

Figure 3-12 Rear panel of the USG2230/2260 basic configuration

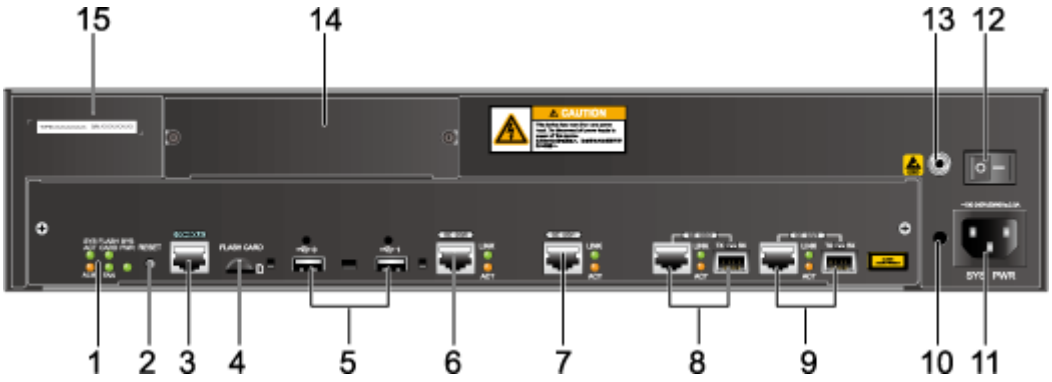
3.1.4 Product Appearance of the USG5100 Series

USG5100 series includes USG5120 and USG5150. Each device consists of an integrated chassis and expansion interface cards.

- The USG5120 provides only AC models. Each device is of 2 U height and provides four MIC slots and four FIC slots. The power supply and fan modules are not hot-swappable and fixed in the USG5120.
- The USG5150 provides only AC models. The USG5150 can house two AC modules that works in load balancing mode. Each device is of 3 U height and provides four MIC slots and six FIC slots. The power supply and fan modules of the USG5150 are hot-swappable.

Front Panel of the USG5120

Figure 3-13 Front panel of the USG5120



1. Indicator	2. Reset button	3. Console port	4. microSD card slot
5. USB port	6. 10/100/1000M Ethernet port 0	7. 10/100/1000M Ethernet port 1	8. GE combo port 2
9. GE combo port 3	10. Locker hole	11. Power socket	12. Power switch
13. ESD jack	14. Dust-proof panel	15. ESN	

Rear Panel of the USG5120

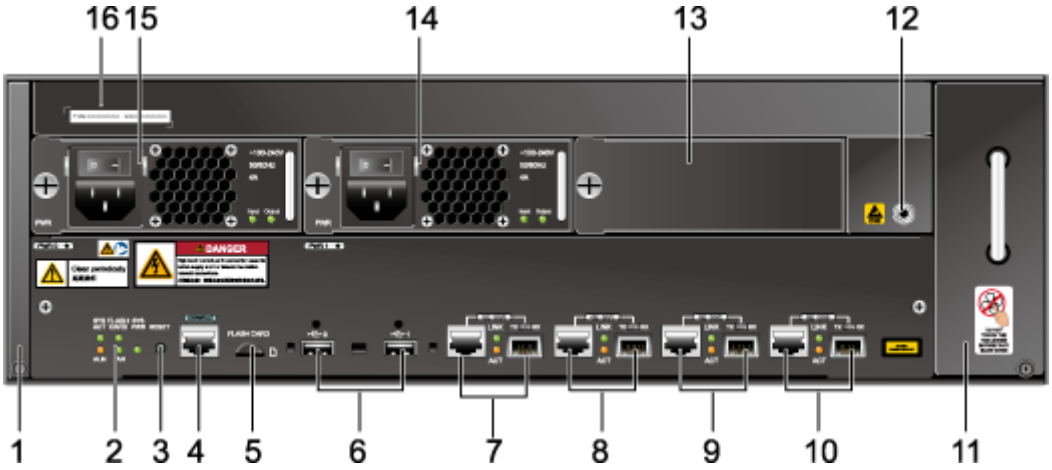
Figure 3-14 Rear panel of the USG5120

1. MIC1/DMIC1 2. MIC2/DMIC2 3. MIC3

4. MIC4	5. FIC5/DFIC5	6. FIC6/DFIC6
7. FIC7/DFIC7	8. FIC8	9. Slot identifier
10. Ground terminal		

Front Panel of the USG5150

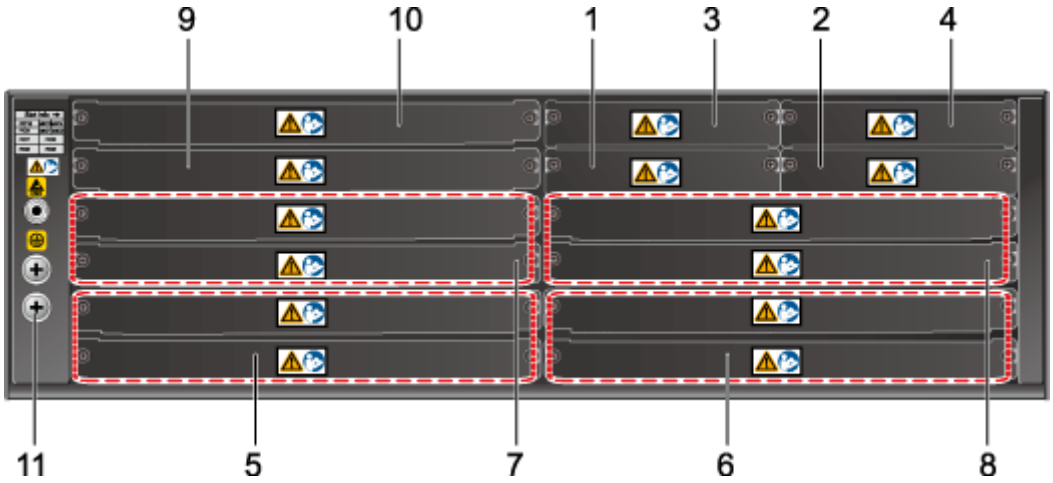
Figure 3-15 Front panel of the USG5150



1. Air filter	2. Indicator	3. One-button recovery button
4. Console port	5. microSD card slot	6. USB2.0 port
7. GE combo port 0	8. GE combo port 1	9. GE combo port 2
10. GE combo port 3	11. Fan frame	12. ESD jack
13. Dust-proof panel	14. Power module 1	15. Power module 0
16. ESN		

Rear Panel of the USG5150

Figure 3-16 Rear panel of the USG5150



1. MIC1/DMIC1	2. MIC2/DMIC2	3. MIC3	4. MIC4
5. FIC5/DFIC5	6. FIC6/DFIC6	7. FIC7/DFIC7	8. GE combo port 2
9. FIC9	10. FIC10	11. Ground terminal	

3.1.5 Product Appearance of the USG5500 Series

The USG5500 series includes the USG5520S, USG5530S, USG5530, USG5550, and USG5560. The USG5520S, USG5530S and USG5530 provide only AC models. The USG5550 and USG5560 provide both AC and DC models. Each device can house two DC or AC modules that works in load balancing mode. The power supply and fan modules of the device are hot-swappable.

Front Panel of the USG5520S/5530S

Figure 3-17 shows the front panel of the USG5520S/5530S.

Figure 3-17 Front panel of a 1U model

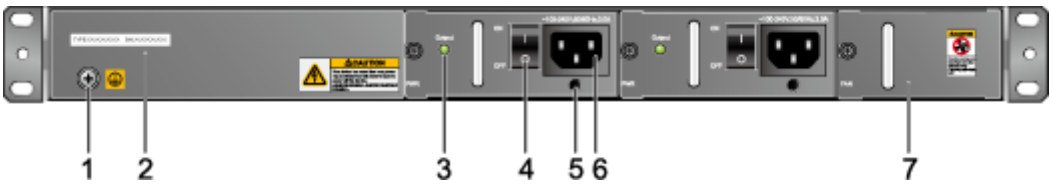
1. ESD jack	2. Reset button	3. Indicator
4. Micro SD card slot (temporarily unavailable)	5. FIC2	6. FIC1/DFIC1
7. Combo port	8. 10/100/1000M Ethernet	9. Management

	electrical port	port
10. Console port	11. USB 2.0 port	

Rear Panel of the USG5520S/5530S

Figure 3-18 shows the rear panel of the USG5520S/5530S.

Figure 3-18 Rear panel of a 1U model

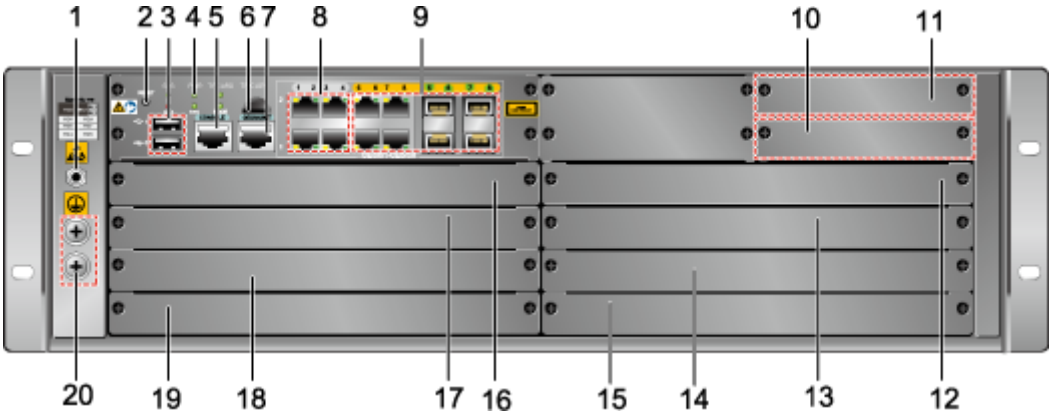


1. Ground terminal	2. ESN	3. Power indicator
4. Power switch	5. AC power cable jack	6. Power receptacle
7. Fan tray assembly		

Front Panel of the USG5530/5550/5560

Figure 3-19, Figure 3-20, and Figure 3-21 show the front panels of the USG5530, USG5550, and USG5560 respectively.

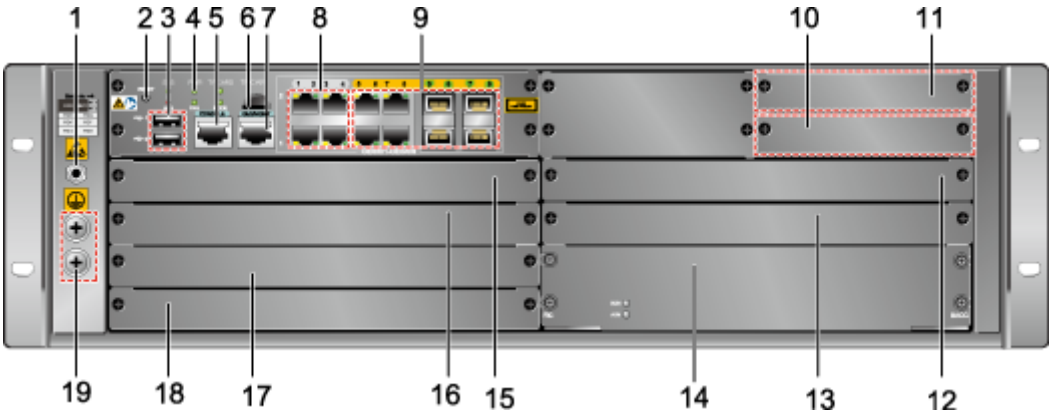
Figure 3-19 Front panel of the USG5530



1. ESD jack	2. Reset button	3. USB 2.0 port
4. Indicator	5. Console port	6. Micro SD card slot (temporarily unavailable)
7. Management port	8. 10/100/1000M Ethernet electrical port	9. Combo port
10. MIC/DMIC2	11. MIC3	12. FIC9

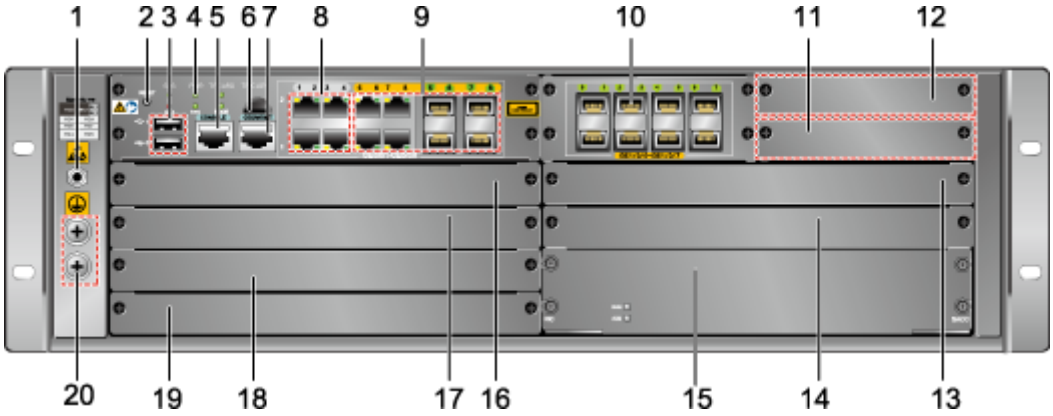
13. FIC/DFIC7	14. Filler panel	15. FIC/DFIC5
16. FIC8	17. FIC/DFIC6	18. Filler panel
19. FIC/DFIC4	20. Grounding terminal	

Figure 3-20 Front panel of the USG5550



1. ESD jack	2. Reset button	3. USB 2.0 port
4. Indicator	5. Console port	6. Micro SD card slot (temporarily unavailable)
7. Management port	8. 10/100/1000M Ethernet electrical port	9. Combo port
10. MIC/DMIC2	11. MIC3	12. FIC9
13. FIC/DFIC7	14. FPGA accelerator	15. FIC8
16. FIC/DFIC6	17. Filler panel	18. FIC/DFIC4
19. Grounding terminal		

Figure 3-21 Front panel of the USG5560



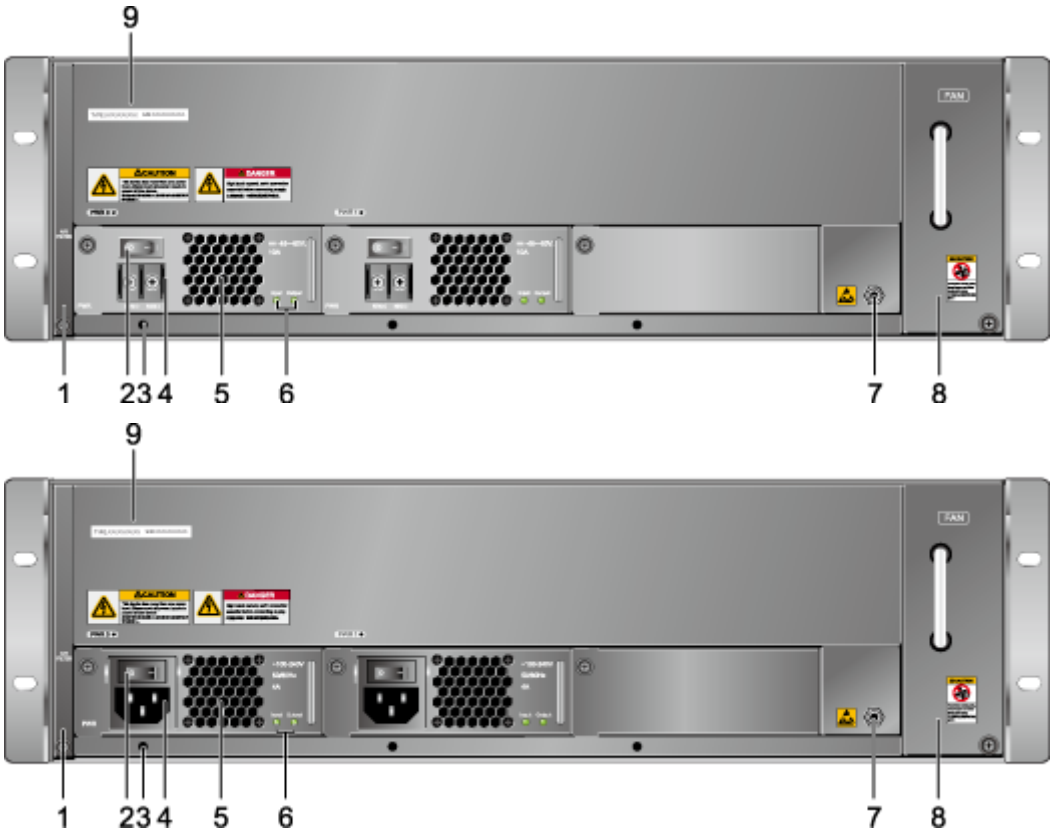
1. ESD jack	2. Reset button	3. USB 2.0 port
4. Indicator	5. Console port	6. Micro SD card slot (temporarily unavailable)
7. Management port	8. 10/100/1000M Ethernet electrical port	9. Combo port
10. 100/1000M optical Ethernet interface	11. MIC/DMIC2	12. MIC3
13. FIC9	14. FIC/DFIC7	15. FPGA accelerator
16. FIC8	17. FIC/DFIC6	18. Filler panel
19. FIC/DFIC4	20. Grounding terminal	

Rear Panel of the USG5530/5550/5560

Figure 3-22 shows the rear panel of the USG5530/5550/5560. The first figure shows a DC model, and the second figure shows an AC model.

NOTE
The USG5530 does not support DC power supply.

Figure 3-22 Rear panel



1. Air filter
2. Power switch
3. AC power cable jack
4. Power receptacle
5. Air filter for the power supply
6. Power indicator
7. ESD jack
8. Fan tray assembly
9. ESN

3.1.6 Expansion Interface Cards and Fixed Ports

Fixed Port

The USG provides fixed ports and supports a wide range of expansion interface cards to provide scalability.

Table 3-1 Fixed port

USG2100	USG2200	USG5120	USG5150	USG5520S/ 5530S/5530/ 5550	USG5560
• One WAN Ethernet interface • Eight LAN	• Two GE combo ports (WAN ports) • One	• Two GE electrical ports (WAN ports) • Two GE	• Two GE electrical ports (WAN ports) • Four GE	• One console port • One 10/100/1000M	• One console port • One 10/100/1000M

USG2100	USG2200	USG5120	USG5150	USG5520S/ 5530S/5530/ 5550	USG5560
Ethernet interfaces • One console port • One full-speed USB port • One Flash interface	console port • Two full-speed USB ports • One microSD card slot	combo ports (WAN ports) • One console port • Two full-speed USB ports • One microSD card slot	combo ports (WAN ports) • One console port • Two full-speed USB 2.0 ports • One microSD card slot	management port • Two USB ports • Four 10/100/1000M Ethernet electrical ports • Four Gigabit combo ports	management port • Two USB ports • Four 10/100/1000M Ethernet electrical ports • Four GE combo ports • Eight 100/1000M Ethernet optical ports

Expansion Interface Card

NOTE
The USG2100 does not support FIC or DFIC interface card.

Table 3-2 Expansion interface card of USG2100/2200/5100

Type	Interface Card	Port	Function
MIC	1 x E1 interface card	One E1 port	-
MIC	1 x CE1 interface card	One CE1 port	-
MIC	1 x ADSL2+ interface card	One ADSL2+ port	Applies to asymmetric rate transmission.
MIC	1 x FE interface card	One 10/100M auto-sensing Ethernet electrical port	-
MIC	5 x FSW interface card	Five 10/100M auto-sensing Ethernet electrical ports	-
MIC	1 x SA interface card	One synchronous/asynchrono	-

Type	Interface Card	Port	Function
		us serial port	
MIC	1 x G.SHDSL interface card	One G.SHDSL port	-
MIC	2 x G.SHDSL interface card	Two G.SHDSL ports	-
MIC	4 x G.SHDSL interface card	Four G.SHDSL ports	-
MIC	2 x SA interface card	Two synchronous/asynchronous serial ports	-
MIC	MIC-3G-WCDMA interface card	Supports 3G connection in WCDMA, and no cable is needed.	Only one 3G interface card (either USB-3G or MIC-3G) can be used on the device at a time. Purchase the interface card based on the network environment.
MIC	MIC-3G-CDMA2000 interface card	Provides CDMA2000 connection.	
MIC	MIC-3G-TD-SCDMA interface card	Provides TD-SCDMA connection.	
MIC	WiFi interface card (The USG2100 does not support this card)	WLAN interfaces provide users with wireless accesses.	-
DMIC	8 x FE+2 x GE interface card	Eight 10/100M auto-sensing Ethernet electrical ports and two 10/100/1000M auto-sensing Ethernet electrical ports	-
FIC	2 x E1 interface card	Two E1 ports	-
FIC	2 x CE1 interface card	Two CE1 ports	-
FIC	4 x E1 interface card	Four E1 ports	-
FIC	4 x CE1 interface card	Four CE1 ports	-
FIC	8 x E1 interface card	Eight E1 ports	-
FIC	8 x CE1 interface card	Eight CE1 ports	-
FIC	1 x GE interface card	One 10/100/1000M auto-sensing Ethernet	-

Type	Interface Card	Port	Function
		electrical port	
FIC	4 x GE interface card	Four 10/100/1000M auto-sensing Ethernet electrical ports	-
FIC	2 x FE+2 x FE combo interface card	Two 10/100M auto-sensing Ethernet electrical ports and two 10/100M combo ports	-
FIC	Electrical bypass interface card (The USG2200 does not support this interface card.)	Four 10/100/1000M auto-sensing Ethernet electrical ports	Enables direct connection between the upstream and downstream devices of the USG, so that the traffic can bypass the USG when the device is faulty or powered off.
DFIC	18 x FE+2 x SFP interface card	Eighteen 10/100M auto-sensing Ethernet electrical ports and two GE optical ports	Layer-2 interface card.
DFIC	16 x GE+4 x SFP interface card	Sixteen 10/100/1000M auto-sensing Ethernet electrical ports and four GE optical ports	Layer-2 interface card.

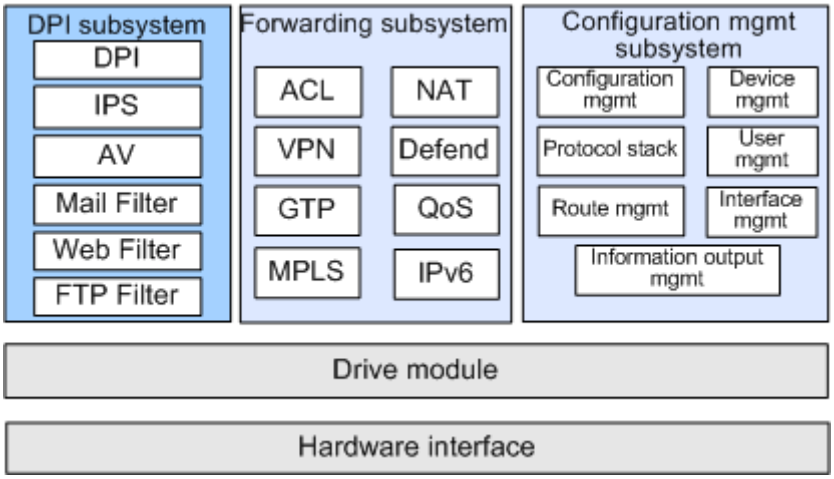
Table 3-3 Expansion interface card of USG5500

Type	Interface Card	Port	Function
FIC	2 x 10-GE optical interface card	Two 10-GE optical ports	-
FIC	2 x 10GE optical+8 x GE electrical interface card	Eight 10/100/1000M auto-sensing Ethernet electrical ports and two 10GE optical ports	-
FIC	8 x GE electrical interface card	Eight 10/100/1000M auto-sensing Ethernet electrical ports	-
FIC	4 x GE electrical bypass interface card	Four 10/100/1000M Ethernet electrical ports	Enables direct connection between the upstream device and the downstream device of the USG when the USG is

Type	Interface Card	Port	Function
			faulty or powered off.
FIC	Optical bypass interface card	Provides two bypass link-layer subcards, with four optical ports on each link-layer subcard.	The bypass link-layer subcard can operate in working or protection mode. In working mode, the subcard diverts the traffic from an upstream device to the USG. After the traffic is processed, the subcard diverts the processed traffic to the downstream device. In protection mode, the USG directly connects the upstream and downstream devices.
FIC	8 x GE optical interface card	Eight GE optical ports	-
DFIC	16 x GE Electrical+4 x GE optical interface card	Sixteen 10/100/1000M auto-sensing Ethernet electrical ports and four GE optical ports	Layer-2 interface card.
DFIC	18 x FE electrical+2 x GE optical interface card	Eighteen 10/100M auto-sensing Ethernet electrical ports and two GE optical ports	Layer-2 interface card.
DFIC	FPGA accelerator	None	Accelerates packet forwarding. Non-first packets are directly forwarded by the accelerator without being processed by the CPU. **NOTE** The FPGA accelerator is not supported on the USG5520S/5530S/5530. The FPGA accelerator is supported on the USG5550/5560 and is delivered with it.
DMIC	2 x 10GE optical interface card	Two 10GE optical ports	**NOTE** The DMIC can be installed only in slot MIC2/DMIC2, and the filler panel of slot MIC3 must be removed.
USB	USB-3G-E180 card	-	WCDMA

Type	Interface Card	Port	Function
USB	USB-3G-EC169/EC169C card	-	CDMA2000
USB	USB-3G-ET128/ET128-2 card	-	TD-SCDMA

3.2 Software Structure



DPI Subsystem

The deep packet inspection (DPI) subsystem examines the application-layer contents of packets to prevent application-layer attacks. The functions of the DPI subsystem include application-layer protocol control, intrusion prevention, anti-virus, mail filter, web filter and FTP filter.

Forwarding Subsystem

The forwarding subsystem forwards packets and supports blacklist, ACL, NAT, VPN, attack defense, fragmentation, GTP, MPLS, and IPv6.

Configuration Management Subsystem

The configuration management subsystem manages the entire system and interacts with users. This subsystem also provides interfaces for configuration, testing, and maintenance. It manages the device, configurations, file systems, logs and alarms, software patches, licenses, and routing.

Drive Module and Hardware Interface

The drive module and hardware interface enable the communication between software and hardware.

4 Service Features

About This Chapter

4.1 Function List

Table 4-1 shows the features available on the USG2110-X/2100/2200/5100/5500.

Table 4-1 Features available on the USG2110-X/2100/2200/5100/5500 series

Category	Description		USG2110-X	USG2100	USG2200	USG5100	USG5500
Firewall functions	ACL and security policy	• Supports unified security policies. • Supports basic and	Y	Y	Y	Y	Y

Category	Description		USG2110-X	USG2100	USG2200	USG5100	USG5500
		advanced ACLs. • Supports time-based ACLs. • Supports MAC-based ACLs. • Supports hardware packet-filtering ACLs. • Supports modification of referenced ACL rules. • Supports blacklist and IP-MAC address binding. • Supports application-layer filtering and stateful inspection. • Supports port mapping.					
	NAT	• Supports NAT and PAT • Supports internal server. • Supports port-level NAT server. • Supports multiple types of NAT ALG.	Y	Y	Y	Y	Y
	Attack defense	• Defends against DDoS	Y	Y	Y	Y	Y

Category	Description		USG2110-X	USG2100	USG2200	USG5100	USG5500
		attacks. • Defends against scanning attacks. • Defends against malformed packet attacks. • Defends against special packet control attacks.					
	TSM interworking	• Supports terminal access control. • Supports multiple privileges. • Supports forced user logout. • Provides the emergency channel function.	Y	Y	Y	Y	Y
	Supports virtual firewall.		Y	Y	Y	Y	Y
	IDS interworking		Y	Y	Y	Y	Y
UTM	Anti-virus	• Supports the scanning of files transmitted through HTTP, SMTP, and POP3. • Supports the local and online update of the virus database daily.	Y	Y	Y	Y	Y

Category	Description		USG2110-X	USG2100	USG2200	USG5100	USG5500
		• Supports the rollback of virus database. • Supports global virus scanning and protocol-specific policy configuration.					
	Intrusion prevention	• Supports in-depth inspection. • Supports the local and online update of the IPS signature database daily. • Supports the rollback of the IPS signature database. • Supports customized IPS policies.	Y	Y	Y	Y	Y
	Web filtering	• Supports Web content filtering. • Supports search engine keyword-based filtering. • Supports the filtering of URLs in HTTP requests to provide refined online behavior management	N	N	Y	Y	Y

Category	Description		USG2110-X	USG2100	USG2200	USG5100	USG5500
		. • Supports URL filtering based on the blacklist, whitelist, and predefined and user-defined categories. • Supports HTTP access logs recording the resources with specified name extensions.					
	Mail filtering	• Supports anti-spam feature. • Supports mail content filtering.	N	N	Y	Y	Y
	FTP filtering	• Supports active and passive modes. • Support FTP command filtering. • Support FTP file filtering. • Supporting restricting file size. • Supports FTP auditing.	N	N	Y	Y	Y
	DPI	• Supports the DPI rule base query.	Y	Y	Y	Y	Y

Category	Description		USG2110-X	USG2100	USG2200	USG5100	USG5500
		The DPI rule base covers a wide variety of protocol signatures. • Supports the online and local update of the DPI rule base. • Supports time-based control policy: For example, IM applications such as MSN can be blocked during working hours but allowed during off hours. • Supports protocol-based traffic limiting and connection number limiting to control gaming, stock trading, P2P, IM, and VoIP traffic.					
MPLS VPN	• Supports BGP/MPLS IP VPN. • Supports L2TP VPN. • Supports IPSec VPN. • Supports GRE VPN. • Supports SSL VPN. • Supports CA certificate.		Y	Y	Y	Y	Y
User	Network	• Supports	Y	Y	Y	Y	Y

Category	Description		USG2110-X	USG2100	USG2200	USG5100	USG5500
authentication	user management	layered and grouped user management. • Supports user authentication scope management. • Supports local authentication, RADIUS server authentication, LDAP server authentication, AD server authentication, and Single Sign-on (SSO).					
	User access management	• Supports RADIUS, including Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP). • Supports PPP and login user authentication. • Supports local authentication. • Supports	Y	Y	Y	Y	Y

Category	Description		USG2110-X	USG2100	USG2200	USG5100	USG5500
		multiple Internet Service Providers (ISPs).					
Access	Ethernet	• Supports Layer-2 and Layer-3 Ethernet ports. • Supports the switch between Layer-2 and Layer-3 Ethernet ports. • Supports Layer-3 Ethernet ports.	Y	Y	Y	Y	Y
	Eth-Trunk	• Supports Layer-2 and Layer-3 Eth-Trunk interfaces. • Supports Layer-3 Eth-Trunk subinterfaces.	Y	Y	Y	Y	Y
	VLAN	• Supports the forwarding through Vlanif interfaces. • Supports access ports. • Supports trunk ports. • Supports hybrid ports.	Y	Y	Y	Y	Y
	PPPoE	• PPPoE Client • PPPoE Server	Y	Y	Y	Y	Y

Category	Description		USG2110-X	USG2100	USG2200	USG5100	USG5500
	Link aggregation		N	N	Y	Y	Y
	DCC		Y	Y	Y	Y	Y
	HDLC		Y	Y	Y	Y	N
	Port isolation		N	Y	Y	Y	Y
	MSTP		N	Y	Y	Y	Y
	3G		Y	Y	Y	Y	Y
	WLAN		Y	Y	Y	Y	N
	SA		N	Y	Y	Y	N
	E1/CE1		N	Y	Y	Y	N
	ADSL2+		Y	Y	Y	Y	N
	SHDSL		N	Y	Y	Y	N
	PPP/MP		Not supporting MP	Y	Y	Y	Not supporting MP
IP service	ARP	• Static ARP • Dynamic ARP • ARP proxy • Gratuitous ARP	Y	Y	Y	Y	Y
	DNS	• Supports local static DNS. • Supports DNS client. • Supports DNS proxy. • Supports dynamic DNS (DDNS).	Y	Y	Y	Y	Y
	DHCP	• Operates as a DHCP server. • Operates as a DHCP client. • Operates as a DHCP	Y	Y	Y	Y	Y

Category	Description		USG2110-X	USG2100	USG2200	USG5100	USG5500
		relay. • Supports DHCP snooping.					
	IPV6	• Supports IPv6 PPPoE • Supports IPv6 DNS. • Supports DHCPv6. • Supports IPv6 over IPv4 tunnels. • Supports IPv4 over IPv6 tunnels. • Supports NAT64. • Supports IPv6 ACL. • Supports IPv6 ASPF. • Supports IPv6 URPF. • Supports IPv6 QoS.	Y (Not supporting NAT64)	Y (Not supporting NAT64)	Y	Y	Y
Routing	IPv4 routing	• Supports static routing. • Supports dynamic routing protocols such as RIP, OSPF, BGP, and IS-IS. • Supports routing policies and route recursion. • Supports IP unicast policy-based	Y	Y	Y	Y	Y

Category	Description		USG2110-X	USG2100	USG2200	USG5100	USG5500
		routing					
	IPv6 routing	• Supports static routing. • Supports dynamic routing protocols such as RIPng, OSPFv3, and BGP4+, and IS-ISv6. • Supports routing policies and route recursion.	Y	Y	Y	Y	Y
IP multicast	• Supports IGMP, IGMP snooping, PIM-DM, PIM-SM, and MSDP. • Supports static multicast.		Y (Not supporting IGMP snooping)	Y (Not supporting IGMP snooping)	Y	Y	Y
Maintenance and reliability	• Supports port mirroring. • Supports remote packet capture. • Supports dual-system hot backup. • Supports load balancing. • Supports link-group. • Supports 1+1 power redundancy. • Supports the bypass interface card • Supports BFD		Y (Not supporting bybass interface cards or BFD)	Y (Not supporting bybass interface cards or BFD)	Y	Y	Y
	Flexible upgrade methods	• Upgrade through FTP. • Upgrade through TFTP. • Upgrade through web pages.	Y	Y	Y	Y	Y

Category	Description		USG2110-X	USG2100	USG2200	USG5100	USG5500
		• Upgrade through BootROM. • Upgrade through USB disks.					
QoS and traffic control	• Supports traffic policing. • Supports traffic shaping. • Supports Limit Rate (LR). • Supports congestion management. • Supports congestion avoidance. • Supports Hierarchical Quality of Service (HQoS). • Supports IP address-based traffic control, including traffic control on individual IP address and multiple IP addresses, which ensures minimum bandwidth and supports idle time bandwidth borrowing.		Y	Y	Y	Y	Y
System management	Information center	Manages and exports logs, alarms, and debugging information.	Y	Y	Y	Y	Y
	SNMP	• Supports SNMP v1 • Supports SNMP v2c • Supports SNMP v3	Y	Y	Y	Y	Y
	Web management	• Supports Web-based device management through HTTP. • Supports Web-based device	Y	Y	Y	Y	Y

Category	Description		USG2110-X	USG2100	USG2200	USG5100	USG5500
		management through HTTPS.					
	NTP	• Supports NTP client/server mode. • Supports NTP symmetric peer mode. • Supports NTP broadcast on LANs. • Supports NTP multicast mode. • Supports NTP v3 and is compatible with NTP v1 and NTP v2.	Y	Y	Y	Y	Y
	Netstream		Y	Y	Y	Y	Y
	NQA		Y	Y	Y	Y	Y
	CWMP (TR-069)		Y	Y	Y	Y	N

4.2 Security Features

NAT

NAT is a process that converts the IP address in the IP packet header into another IP address.

- Address Translation

  Address translation facilitates access to external networks (public IP addresses) by internal networks (private IP addresses). Through NAT, many private IP addresses can be translated into a few public IP addresses, which slows down the exhaustion of IP addresses.

  Address translation is classified into:

  – IP address translation based on the address pool

- Address translation by using different policies according to different addresses
- Port Address Translation (PAT) based on addresses and ports (port number of TCP or UDP)
- Address translation based on ACL rules
- Port-level address translation

- NAT Internal Server

  NAT hides the structure of the internal network, which shields the internal host. In actual applications, however, the chance that external users access the internal host may be needed, such as providing a WWW server or an FTP server. Through NAT, internal servers can be flexibly added.

  NAT of the USG series can enable external network users to access internal servers. When external users access internal servers, the following operations are required:

  - The USG series translate the destination IP address of request packets of external users into the private address of the internal server.
  - The USG series translate the source IP address (private address) of reply packets of the internal server into the public address.

  The USG series can provide external users with multiple servers of the same type, such as multiple Web servers.

- Multiple NAT ALGs

  For certain special protocols, such as Internet Control Message Protocol (ICMP) and File Transfer Protocol (FTP), the data part in these packets may contain IP addresses or port information. Such contents cannot be translated through NAT. In this case, problems may occur.

  The USG series support the application of Application Level Gateway (ALG) in NAT.

  Through registration, NAT supports multiple NAT ALGs, including:

  - NAT ALG that supports FTP
  - NAT ALG that supports H.323 (including T.120, RAS, Q.931, and H.245)
  - NAT ALG that supports ICQ protocol
  - NAT ALG that supports the Internet Locator Service (ILS) protocol
  - NAT ALG that supports the Real-Time Streaming Protocol (RTSP)
  - NAT ALG that supports the Media Gateway Control Protocol (MGCP)
  - NAT ALG that supports the Multimedia Messaging Service (MMS) protocol
  - NAT ALG that supports the Point to Point Tunneling Protocol (PPTP)
  - NAT ALG that supports Tencent QQ
  - NAT ALG that supports the NetBIOS over TCP (NBT)
  - NAT ALG that supports the Session Initiation Protocol (SIP)
  - NAT ALG that supports the Internet Control Message Protocol (ICMP)
  - NAT ALG that supports the SQL.NET protocol
  - User-defined NAT ALG

  NAT can support special protocols through registration. Therefore, the software can be better extended and can support new protocols without changing the architecture.

ACLs

ACL is an important method of data control on the device, and applies to packet filtering, Network Address Translation (NAT), IPSec, Quality of Service (QoS), and policy-based

routing. The routing device defines a series of rules to filter packets and therefore determine which packets can pass through. These rules are defined by the ACL.

An ACL consists of a series of orderly rules containing **permit** or **deny** clauses. These rules cover source IP addresses, destination IP addresses, and port numbers of packets. The ACL classifies packets through these rules. After the rules are applied to the interface of a routing device, the device determines which packets can be received and which should be denied according to the ACL.

- Basic ACLs that filter packets based on source IP addresses.
- Advanced ACL that filter packets based on source and destination IP addresses, source and destination ports, and protocols.
- MAC address-based ACLs that filter packets or Ethernet frames based on source and destination MAC addresses, and types and priorities of data frames.

The USG uses the fast flow classification algorithm to ensure that ACL processing does not compromise system performance or forwarding speed, even when there are tens of thousands of ACL rules.

ASPF

The USG also uses Application Specific Packet Filter (ASPF) to filter packets based on their connection status. ASPF examines the application-layer protocols of packets and determines to forward or discard the packets based on the session information. ASPF also blocks harmful Java Applets and ActiveX controls.

Stateful Inspection

As an advanced filtering technology, stateful inspection inspects the application-layer protocol information and monitors the status of connection-oriented application-layer protocols. The USG maintains a session for each connection and determines to forward or discard packets according to the session information.

Stateful inspection incorporates the fast speed and flexibility of packet filtering and the security benefits of proxy firewalls. The USG uses the latest stateful inspection technology to provide high-performance security defense and packet processing.

Virtual Firewall

The USG supports multi-instance solutions to provide services for multiple small private networks. The USG can be logically divided into multiple virtual firewalls to provide separate security services for multiple small private networks. Carriers can use this feature of the USG to lease network security services.

Each virtual firewall can be bound to a VPN instance to provide separate VPN routes for different private networks. Currently, the USG supports multiple instances of IPSec, L2TP, NAT, security zone, ACL, session, blacklist, and routing.

Blacklist for Filtering Malicious Hosts

The USG discards all the packets from blacklisted users to protect legitimate users. Upon detecting suspicious activities from an IP address, the USG automatically adds the IP address to the blacklist and discards the subsequent packets from the IP address.

Blacklist entries can also be added manually and associated with ACLs. After a packet hits a blacklist entry, the USG searches for the ACLs associated with the blacklist entry and determines to forward or discard the packet according to the ACLs.

Blacklists only restricts IP addresses. Therefore, using blacklists is a fast way to block the packets from suspicious IP addresses.

IP-MAC Address Binding

IP-MAC address binding is an effective way to prevent IP spoofing attacks.

The USG supports IP-MAC address binding.

- If the source IP address of a packet is not the one bound to the source MAC address, the packet will be discarded.
- If the destination IP address of a packet is the one bound to the source MAC address, the packet will be forwarded.

Attack Defense

- Defense against DDoS attacks

  The USG can detect DDoS attacks, prevent DDoS them by discarding the attack packets or taking other actions, and log the attack events. The DDoS attacks that can be detected and prevented by the USG include SYN flood attack, UDP flood attack, ICMP flood attack, ARP flood attack, SIP flood attack, HTTP flood attck, and connection flood attack.
- Defense against scanning and sniffing

  By scanning and sniffing, attackers can obtain the information about the services and vulnerabilities on target hosts for subsequent intrusion. The USG can intelligently and efficiently detect such scanning and sniffing packets through comparison and analysis.
- Defense against other attacks

  The USG can also prevent other attacks such as IP spoofing, attacks by taking advantage of the IP source routing option and IP record route option, and network topology sniffing by using tracert tools to secure network access.

GTP

The USG GTP uses UDP to transport packets. On a GPRS network, the USG can serve as a Gn, Gp, or Gi interface.

The USG delivers the following functions based on its location on the network:

- Serves as a Gn interface to filter out malicious packets to protect the NEs on the same Public Land Mobile Network (PLMN).
- Serves as a Gn interface to filter out malicious packets from other PLMNs when a PLMN is connected to other PLMNs to protect the NEs on the PLMN.
- Serves as a Gi interface to filter out malicious packets from external IP networks when a PLMN is connected to external IP networks to protect the NEs on the PLMN.
- Defends against GTP overbilling attacks.

4.3 UTM

The Huawei provides a powerful security service center which facilitates the online update of the IPS signature database and the virus database. The IPS signature database and the virus database enable the USG to effectively identify threats and vulnerabilities in network applications, protecting customers from threats such as Web sites with malicious codes, viruse-infected mails, Trojan horses, backdoor attacks, and illegitimate Web site accesses of employees.

Anti-Virus

The USG scans Web access and email traffic for viruses and forwards the traffic only if no virus is detected. The USG can scan compressed files of multiple formats, packed files, and attachments in emails to prevent virus spread.

The USG can scan files transmitted through HTTP, SMTP, and POP3. You can customize anti-virus scanning polices to accommodate different protocols and networks. For example, you can enable or disable anti-virus scanning for FTP, DNS, etc., configure response mode, and restrict the size and types of files to be scanned. Upon detecting a virus, the USG notifies users by using emails or pushing a Web page. Scanning policies can be applied between desired security zones to avoid the impact of global scanning on performance.

The USG supports manual or scheduled update of the virus database from the security service center. If the USG cannot be connected to the security service center on the Internet, you can download the update package in other ways, upload the update package to the USG, and update the virus database offline. The virus database can be rolled back if necessary.

IPS

The IPS monitors traffic status, detects intrusion by using in-depth packet analysis, and takes actions according to the defined policies.

Conventional firewalls cannot inspect the application-layer data (such as HTTP) in packets. However, IPS can perform in-depth packet analysis, detect intrusion, and take actions according to the configurations. The IPS can also log intrusion events in real time for future auditing.

The IPS policies on the USG can be customized to accommodate your specific situations.

The IPS can reassemble fragments and TCP flows before inspection. Therefore, attackers cannot bypass the IPS inspection by fragmenting packets. The IPS can also identify application protocols using ephemeral ports, improving the intrusion detection ratio. The IPS also supports protocol analysis and signature inspection to detect attacks such as worm, Trojan horses, scanning, and spyware. You can also use command lines or Web pages to check the attack behaviors, as SQL injection attacks and Java script attacks, that can be detected by the signature database, the description about the attack identified by each signature, and the impact of the attacks.

In in-line deployment of the USG, the IPS can work in protection or alerting mode. In protection mode, the IPS can block attack traffic. In alerting mode, the IPS does not block any traffic and only logs the events and sends alarms to facilitate traffic analysis without any impact on network traffic.

The IPS signature database supports manual and scheduled update to respond rapidly to emerging attacks. If the USG cannot be connected to the security service center on the Internet, you can download the update package in other ways, upload the update package to

the USG, and update the virus database offline. The IPS signature database can be rolled back if necessary.

Mail Filtering

- Anti-spam (RBL filtering)

  RBL filtering blocks spam based on local blacklist, local whitelist, and dynamically updated blacklist provided by a third-party organization. RBL filtering filters the mails transferred through SMTP based on the source IP addresses of the SMTP connections.

- Mail content filtering

  The mail content filtering function monitors the mail address, subject, body, attachment size, attachment name, or attachment name extension when an intranet user sends or receives mails through the Webmail or SMTP/POP3 client to prevent the leak of sensitive data.

Web Filtering

Web filtering includes URL filtering, search engine keyword-based filtering, and Web content filtering.

- URL Filtering

  Visiting illegitimate Web sites not only reduces work efficiency but also compromises network security. The URL filtering function of the USG filters URL requests to ensure that users can access only allowed network resources.

  The URL filtering function is described as follows:

  - Supports URL filtering based on user-defined local URL blacklists and whitelists.
  - Supports URL filtering based on the filtering policies and the URL classification at the security service center.
  - Supports fine-grained URL filtering policies based on time and IP address categories.
  - Supports the binding of access policies to the URL categories, user groups, and time ranges.
  - Supports the pushing of user-defined notification Web pages when URLs are blocked.
  - Supports the logging of URL requests, IP addresses of requesting users, and URL access time for future audit. The USG can audit and analyze the logs on the eLog server and list the top N most visited Web sites by internal users and top N internal users who access Web sites most frequently.

- Search engine keyword-based filtering

  Search engine keyword-based filtering filters configured search engine keywords. The search engines supported are Google, Yahoo, Bing, and Baidu. The administrators can specify the keywords to be filtered on the USG to prevent the users from accessing the searching results that matched the entered keywords when the users search the keywords on the Internet.

- Web content filtering

  Web content filtering can control the Web content that transmitted through HTTP. The items can be controlled include:

  - Web page keyword filtering: Filters the Web page contents based on keywords.
  - Forum posting keywords filtering: Filters the contents posted by intranet users on BBS and forums based on keywords.

- Web page file (including figures, and videos) name filtering: Filters the uploaded and downloaded files based on file names.
- Web page file (including figures, and videos) name extension filtering: Filters the uploaded and downloaded files based on file name extensions.
- File size filtering: Filters the uploaded and downloaded files transmitted through HTTP based on the file size.

FTP Filtering

The FTP file transfer function is vital to network information sharing. If the FTP upload and download are not controlled, threats are likely to exist on the intranet. FTP filtering can filter the FTP operations, file names, file name extensions, and file sizes of uploaded and downloaded files.

Overload Protection

You can enable overload protection on the USG if you prioritize services over security, or disable it if you prioritize security over services. When overload protection is enabled and the traffic exceeds the processing capability of the UTM module, the excess traffic is directly forwarded without any security inspection. When overload protection is disabled and the traffic exceeds the processing capability of the UTM module, the excess traffic is discarded to ensure security.

DPI

The USG uses the Deep Packet Inspection (DPI) technology to perform in-depth inspection on packets, identify application-layer protocols, and control the traffic of specific types. The USG analyzes packets, compares them with the signatures in the DPI rule base, identifies online gaming, stock trading, P2P, IM, and VoIP traffic, and takes actions to control the traffic according to the application type and associated polices.

- Supports the DPI rule base query. The DPI rule base covers a wide variety of protocol signatures.
- Supports the online and local update of the DPI rule base.
- Supports time-based control policy to block some applications such as MSN during working hours but allow them during off hours.
- Supports the control over online gaming, stock trading, P2P, IM, and VoIP traffic.
- Supports user-defined rules to permit or block traffic (such as online gaming, stock trading, or P2P traffic) as needed.

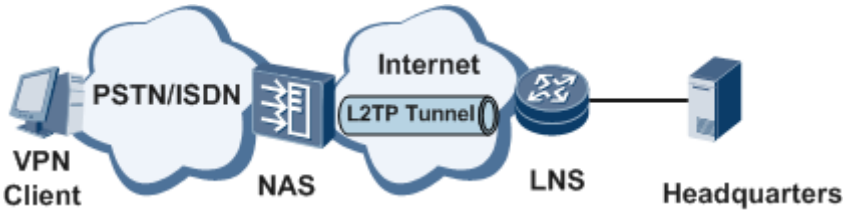
4.4 Features of MPLS and VPN

L2TP

The USG supports constructing a VPDN by using L2TP and a VPN by using the dialing function of public networks (such as ISDN and PSTN) and access networks. The USG provides access services, small ISPs, and mobile business personnel.

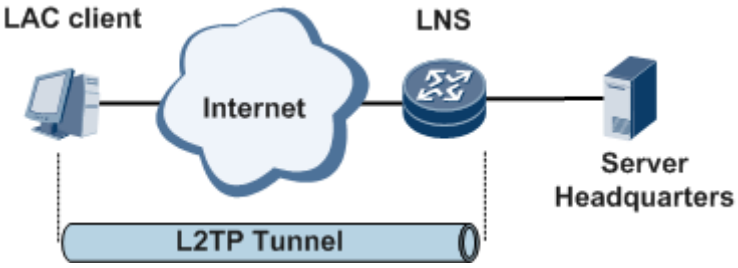
As a LNS or LAC, the USG supports the following three typical tunnelling modes:

Figure 4-1 Schematic diagram of the L2TP tunnel in NAS-initialized mode



As shown in Figure 4-1, the remote system dials up to the LAC through the PSTN/ISDN. Then the LAC (NAS) initiates a request for establishing a tunnel with the LNS through the Internet. The LNS assigns private IP addresses to dialing users. The authentication of remote dialing users can be implemented either by the proxy at either the LAC or LNS side.

Figure 4-2 Schematic diagram of the L2TP tunnel in Client-initialized mode



As shown in Figure 4-2, the LAC client can directly initiate a request for establishing a tunnel with the LNS, but not through an independent LAC. After receiving the LAC client's request, the LNS authenticates the user name and the password of the LAC customer, and then allocates a private IP address for the LAC client.

Proactive dial-up of the LAC: The user can run commands to establish a permanent L2TP session between the LAC and LNS. The LAC uses the user name stored locally to establish a permanent L2TP tunnel with the LNS through the VT interface. In this case, the L2TP tunnel is equivalent to a physical link, with the VT interface as the egress. The connection between the user and the LAC can be an IP connection, so that the LAC can forward the IP packets of the user to the LNS.

IPSec

The IP Security (IPSec) protocol suite, consisting of a series of protocols defined by IETF, provides a high-quality, interactive and cryptology-based security protection mechanism for IP packets. Specific communication parties guarantee the confidentiality, integrity, authenticity, and anti-replay of packets transmitted on the networks by taking measures such as encryption and data source verification at the IP layer.

The USG provides IPSec mechanisms through hardware, and provides secure communication parties with services such as access control, integrity, data source authentication, anti-replay, encryption, and data flow classification like critical data, voice and video, and encryption. Through Authentication Header (AH) and Encapsulating Security Payload (ESP), the USG protects IP data packets or upper layer protocols like voice and video. The USG supports two encapsulation modes: transmission mode and tunnelling mode, as shown in Figure 4-3.

Figure 4-3 Schematic diagram of the IPSec tunnel

The USG also supports the IPSec tunnel negotiation using the IKEv2 protocol. The IKEv2 protocol reserves basic functions of the IKE and overcomes the problems found during IKE researches. Moreover, in view of simplicity, efficiency, security, and robustness, relevant IKE documents are replaced by RFC4306. By minimizing core functions and default password algorithms, IKEv2 greatly improves the interoperation capability among different IPSec VPNs.

Compared with the traditional IKE, the advantages of IKEv2 are as follows:

- Creating one IKE SA and a pair of IPSec SAs through negotiation with four messages, improving the negotiation efficiency.
- Deleting the data structures that are difficult to understand and confusing, including DOI, SIT, and domain identifiers.
- Repairing many cryptographic vulnerabilities, improving the security.
- Defining payloads for specific traffic to share certain functions of the ID payload, increasing the flexibility of the protocol.
- Supporting EAP authentication, improving the flexibility and expansibility of the authentication mode.

The USG IPSec supports CA certificate.

The USG not only provides secure transmission tunnels of high reliability for users through the IPSec, but also supports the combination of the IPSec, L2TP, and GRE to construct multiple VPN applications as follows:

- L2TP over IPSec VPN
- GRE over IPSec VPN

GRE

The USG series can encapsulate certain network layer protocol packets by using the Generic Routing Encapsulation (GRE) protocol. Thus, the encapsulated packets are transmitted through another network layer protocol.

GRE can serve as the Layer 3 tunnel protocol of the VPN, and adopt the tunnel technology among the protocol layers. A tunnel is a virtual point-to-point connection between equipments located in headquarters and branches. It can be regarded as a virtual interface that supports only point-to-point connections. This virtual interface provides a tunnel through which encapsulated data packets can be transmitted. At both ends of a tunnel, data packets are encapsulated or decapsulated.

The USG supports the encapsulation of certain network layer protocol packets by using the Generic Routing Encapsulation (GRE) protocol. In this manner, the encapsulated packets are transmitted carried by another network layer protocol.

SSL VPN

- Virtual Gateway

  In the USG series, the channel established by the SSL VPN module is called a virtual gateway. The USG series provide users with SSL VPN services through virtual gateways. As a physical entity, the USG series can function as multiple logically independent gateways by using the virtual gateway technology. The configurations and services of these virtual gateways are independent of each other, thus meeting the requirements of multiple enterprises or branches of one enterprise.

  For example, a large enterprise has multiple branches, each of them has their own staff. Resources and services accessible for these branches are different. Each branch has specific access control rules. In this case, one virtual gateway is assigned to each branch. Each virtual gateway is under individual management and can be configured with its own users, resources, and policies, functioning as an independent access system. It seems that each branch has its own gateway, which works efficiently and securely as an independent gateway.

  The virtual gateways are classified into the following types based on the IP address and domain name:

  - Exclusive virtual gateway

    An exclusive virtual gateway has one or multiple IP addresses and domain names exclusively.

  - Shared virtual gateway

    Multiple virtual gateways share the same IP address and the same parent domain name. Different virtual gateways are identified by sub-domain names.

- Web Proxy

  Web proxy can provide the relay service for the communications between the external client and the Web server on the internal LAN, thus protecting the Web server on the internal LAN by not exposing it to the external attackers. This provides the Web server with ideal security protection.

  Web proxy enables users to use the USG series to securely access internal Web resources, including the Web mail and Web servers. The Web proxy uses the Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) forwards the access request HTTPS from a remote browser to the internal Web server, and then transmits the response of the server to the terminal user.

  Users can access the Web resources only if the control is installed on the Web page of the virtual gateway client of the USG series.

- Network Expansion

  The network expansion function helps realize access to all IP-based services on the internal network by setting up Secure Socket Layer (SSL) tunnels. Users can easily realize remote access to internal network resources just like they access a LAN. The network expansion function is applicable to a wide range of complex services.

  Users can use the network expansion function in two ways; that is, users can log in to the client of the USG series and install the ActiveX control to enable the network expansion function. Alternatively, users can download and install the network expansion client software.

  The network expansion function supports the following access modes:

  - Full tunnel

    In this mode, users only connect with the USG series and can only access the intranet.

  - Split tunnel

In this mode, users can both realize remote access to the intranet securely through the USG series and access the local subnets.

- Manual tunnel

  In this mode, users can access the specific resources on the intranet, the local subnet, and various resources on the Internet.

- Port Forwarding

  The port forwarding service, as a non-Web application, provides secure access based on Transmission Control Protocol (TCP) applications.

  Port forwarding uses the ActiveX control installed on the client to listen to the TCP requests initiated by users. The ActiveX control encrypts the intercepted data flows with SSL, and then transmits them to the USG series. The USG series decrypt and resolve these data flows, and then transmit them to the corresponding application server. Port forwarding controls user access at the application layer by determining whether to provide applications such as Telnet, remote desktop, File Transfer Protocol (FTP), and Email.

  The USG series support the following applications:

  - Single-port and single-server applications such as MS RDP, Telnet, SSH, and Virtual Network Computing (VNC)
  - Single-port and multi-server applications such as Lotus Notes
  - Dynamic port applications such as FTP and Oracle
  - Multi-port applications such as Email

- File Sharing

  File sharing enables users to access shared resources on servers running on different file systems, such as the Windows system supporting the Server Message Block (SMB) and the Linux system supporting the Network File System (NFS) in the form of Web pages.

  Users can create and browse the directory, and download, upload, rename, and delete files on the internal file system directly with the browser. File sharing function enables users to easily realize the preceding operations just as on the local file system.

MPLS

MPLS is a new technology that combines the advantages of simple signaling of IP technologies and the high efficiency of the ATM switching engine. MPLS VPN can break down the existing IP network into virtual networks logically isolated from each other and is widely used in VPN, TE, and QoS.

All the devices involved in MPLS forwarding in an MPLS domain must be configured with basic MPLS functions. In addition, you can configure other MPLS features only after configuring basic MPLS functions. The static Label Switched Path (LSP) cannot be established through label distribution protocols, and requires manual configuration by the administrator. When configuring the static LSP, the administrator needs to assign labels to LSRs manually. The principle of the manual configuration is that the value of the outbound label at the last node must be equal to that of the inbound label at the next node.

LSRs on the static LSP cannot sense the situation of the whole LSP. Therefore, LSP is a local concept.

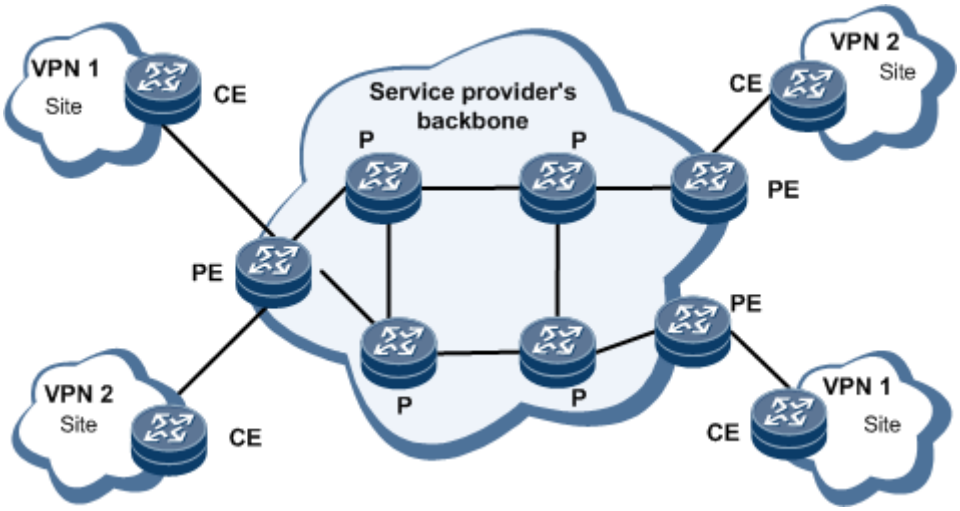
The LDP is a way of creating dynamic LSPs. If strict control of the LSP establishment or the deployment of the traffic project on the MPLS network is not required, you are recommended to adopt LDP to create LSPs.

BGP MPLS IP VPN

The BGP/MPLS IP VPN is a PE-based L3VPN technology of Provider Provisioned VPN (PPVPN) solutions. It employs BGP to advertise VPN routes and MPLS to forward VPN packets on the backbone networks of service providers.

BGP/MPLS IP VPN provides flexible networking with excellent scalability, and easily supports MPLS QoS. Therefore, it is applied more and more widely.

Figure 4-4 Schematic diagram of the L3VPN tunnel



The model of the BGP/MPLS IP VPN comprises the CE, PE and P.

- The Customer Edge (CE): indicates the device at the border of the user's network, and is directly connected to the service provider network through an interface. The CE can be a USG, a switch, or a host. Generally, the CE cannot "sense" the existence of the VPN, and does not need to support MPLS.
- Provider Edge (PE): indicates the device at the border of the service provider network, and is directly connected to the CE. On the MPLS network, all processing related to the VPN is on the PE.
- Provider (P): indicates the backbone device on the service provider network, and is not directly connected to the CE. The P only needs to support basic MPLS forwarding and does not maintain VPN-related information.
- Site: indicates a group of IP addresses with connectivity, which can be realized without the service provider network. The site connects to the service provider network through the CE. One site contains multiple CEs, but one CE only belongs to one site.

4.5 User Management

Network User Management

Network users indicate the users who access the network resources through the USG, including the users who initiate network accesses in the intranet, such as intranet PC users and

users on the extranet who initiate access to the intranet resource through the USG, for example employees on business trips.

The network user management function classifies the departments of a company into different levels, adds the intranet users into different user groups, and performs network behavior audit based on the users or user groups, then create the policies based on the users or user groups in a visualized manner. This function enhances usability of the policies created, displays user information in the report, and analyzes the online behaviors to trail and audit certain users instead of certain IP addresses. This function resolves the issue of analyzing the user behaviors whose IP addresses change frequently on the live network.

The network management function supports the creating, deleting, moving, modifying, querying, importing, exporting of users and user groups, binding of IP/MAC addresses, configuring account validity period, creating alias names, generating descriptions, and setting the statuses of the users or user groups.

This function supports the network segment-based non-authentication, password authentication (local authentication servers or third-party authentication servers), and Single Sign-on (SSo). The non-authentication exempts users from authentication based on IP-MAC bindings and IP address segments. The third party authentication servers include RADIUS servers, LADP servers, SecureID servers, AD servers, and the SSo only supports the AD server authentication.

The network user management function supports AD single sign-on, Web session authentication, auto-redirection after successful authentication, redirection to the latest accessed pages, HTTP and HTTPS authentication modes, user-defined maximum failed authentication attempts and lockout duration, and user-defined online user aging time.

The administrators can perform the operations on the online users including viewing, activation, forcing out, lockout, and canceling the lockout.

Access User Management

The access users indicate the users using the PPP connections and the tunnels established. The USG supports local, RADIUS, and HWTACACS authentication and authorization to prevent unauthorized access.

Administrator

An administrator accesses and configures or operates the device through Telnet, SSH, Web, FTP, or the console port. Upon the factory delivery, default administrator account **admin** and password **Admin@123** are provided for the access to the device in three modes, Telnet, Web, and console port.

4.6 Availability

VRRP

The USG series support the Virtual Router Redundancy Protocol (VRRP), and forming backup groups based on the virtual IP address. The hosts on the network communicate with other networks by using the virtual IP address as the IP address of the gateway.

Dual-System Hot Backup

The USG series support the Huawei Redundancy Protocol (HRP). A backup group includes a master device and a backup device. HRP is responsible for delivering key configuration commands and information about session tables from the master device to the backup device, which ensures that the backup device can smoothly take the place of a failed master device and keep up running the services such as Internet, VPN among others.

BFD

Bidirectional Forwarding Detection (BFD) quickly identifies communications faults between systems and reports corresponding faults to upper-level protocols.

To reduce the adverse impacts on services and promote the network availability, communication faults between neighboring devices must be identified rapidly, so that countermeasures can be taken in a timely manner to ensure service continuity.

BFD provides low-overhead and rapid fault detection for the links between adjacent forwarding engines. The faults may occur on interfaces, data links, or even forwarding engines.

BFD provides a single mechanism to perform the real-time detection for any media and protocol layers. It also supports different detection duration and overheads.

Load Balancing

When one server cannot process the access requests of several users, multiple servers can be used to share network traffic. In this case, the USG series can be deployed at the egress of the network where the servers reside. Users only need to access one IP address, and the USG series distribute access traffic to several servers according to the configured algorithm. In this way, the processing capacity of each server is fully exploited and load balancing is accomplished. In addition, the availability of the server is guaranteed and the optimal network scalability is achieved.

The USG series support health check on servers.

Link-Group

Link-group is to bind several physical interfaces to form a logical group. If any of the interfaces in the logical group is faulty, the system changes the status of the other interfaces to down. After all the interfaces recover, the system changes the status of the interfaces to up.

Bypass

The USG5100 and USG5500 uses dedicated bypass interface card. When the device is faulty or powered off, the bypass interface card directly connects the upstream and downstream devices of the USG5500 to ensure service continuity.

4.7 QoS

It is difficult to ensure QoS in the traditional IP network. Because devices in the network handle all the packets equally.

With the rapid development of network technologies and diversification of services, increasingly high requirements are imposed on service quality. These new applications put forward special requirements for bandwidth, delay, and jitter. For example, videoconference and video on demand require high bandwidth, low delay, and low jitter. Telnet stresses on low delay and priority handling in the event of congestion. As new services spring up, the number of requests for the service capability of IP networks has been on the rise. Users expect improved service transmission to the destination and also better quality of services. For example, IP networks are expected to provide dedicated bandwidth, reduce packet loss ratio, avoid network congestion, control network flow, and set the preference of packets to provide different QoS for various services. All these demand better service capability from the network, and QoS is just an answer to the requirements.

Techniques used for the QoS application are as follows:

- Traffic policing

  Discards packets that exceed the configured limit to avoid congestions caused by traffic bursts.

- Traffic shaping

  Buffers the packets that exceed the configured limit and sends them at later timeslots to accommodate the forwarding speed of the downstream device and avoid packet loss.

- Congestion avoidance

  Supports tail drops and Weighted Random Early Detection (WRED) algorithms to discard packets and avoid queue overflow.

- Congestion management

  Supports FIFO queuing, CQ, PQ, and WFQ scheduling algorithms to balance scheduling fairness and the preferential processing of traffic with higher priorities. The QoS features meet the differentiated requirements of services such as data and voice services on latency, jitter, bandwidth, and packet loss ratio to accommodate different services on IP networks.

- Limit rate

  Uses the token bucket for traffic control. If LR is configured on a device interface, all packets to be sent through the interface are processed first by the token bucket of LR. The packets can be sent, if the packets have sufficient tokens in the bucket. Otherwise, the packets are put into QoS queues for congestion management.

- HQoS

  Implements traffic control on users and performs QoS scheduling based on the priority of the service traffic at the same time. QoS cannot implement priorirized traffic service for multiple users on an interface, and HQoS overcomes the defect. The HQoS can prioritize traffic both by users and by service, providing refined services and reducing the maintenance cost of the entire network.

The device also supports the IP-based limiting on the bandwidth and the connection number to control the interzone traffic and optimizes network traffic, guarantees the normal access rates of users, and helps in attack defense.

- Individual IP address-based traffic control

  Limits the bandwidth and the number of the connections initiated from or received by a given IP address matching the conditions.

- Multiple IP address-based traffic control

  Limits the bandwidth and the number of the connections initiated from or received by multiple IP addresses meeting the conditions.

4.8 IP Service

ARP

The Address Resolution Protocol (ARP) is an address resolution mechanism to map an IP address to a MAC address.

Each host or routing device on the LAN has a 32-bit IP address, which is used for all the communication of the host. The assignment of IP addresses is independent on hardware addresses.

On the Ethernet, the host or routing device sends and receives data frames according to the 48-bit MAC address. This MAC address, also called physical address or hardware address, is assigned to the Ethernet when the device is manufactured. Therefore, in the actual internetworking, an address mechanism is required to provide mapping between the IP address and MAC address.

DHCP

DHCP adopts the client/server mode. The client applies for configurations including the assigned IP address, subnet mask, and default gateway to the server. Then the server returns corresponding configuration information according to policies.

As the network is developing rapidly in scale and complexity and network configuration is more and more complicated, the places of PCs are changed (for example, the laptop or wireless network), and the number of PCs exceeds that of available IP addresses. The DHCP emerges in response to these problems.

The USG supports the DHCP server, proxy, and client. The PCs connected to the USG through DHCP can obtain IP addresses and configuration information needed rapidly and dynamically, requiring no manual specification of the administrator.

DNS

TCP/IP not only identifies devices with IP addresses, but also provides a host naming mechanism in character string format (namely, the Domain Name System (DNS)). The DNS adopts a hierarchical naming mode to specify a meaningful name for the device on the network, set the DNS server, and establish mapping relationships between domain names and IP addresses.

The domain name resolution consists of dynamic and static DNS resolution. To resolve domain names, static resolution is preferentially adopted. The dynamic resolution is adopted only if the static resolution fails. Certain common domain names can be added to the static domain name resolution table, which significantly increases the efficiency of domain name resolution.

The USG supports the DNS client and DNS proxy.

The DNS only provides the static mapping relationships between domain names and IP addresses. When the IP address of a node changes, the DNS cannot dynamically update mapping relationships between domain names and IP addresses. In this case, if the domain name is adopted to access the node, the IP address obtained through the domain name resolution is incorrect. As a result, the access fails. The DDNS dynamically updates the mapping relationships between domain names and IP addresses on the DNS server, ensuring that IP addresses obtained through the domain name resolution are correct.

NAT64

NAT64, a transition technology, is applicable to the evolution from IPv4 networks to IPv6 networks which enables the coexistence of and data exchange between IPv6 networks and IPv4 networks.

NAT64 translates the transport addresses between the IPv6 transport addresses (IPv6 addresses with TCP or UDP ports) and IPv4 transport addresses (IPv4 addresses with TCP or UDP ports).

NAT64 also translates the packet headers, TCP, UDP, and ICMP between IPv6 packets and IPv4 packets.

IPv6 over IPv4

During the initial phase of the evolution from IPv4 networks to IPv6 networks, IPv4 networks are deployed on a large scale but IPv6 networks are scattered similar to islands. It is obviously uneconomical to use dedicated lines to connect these islands. The common practice adopts tunneling technologies. Through tunneling technologies, the user can create tunnels on IPv4 networks to connect IPv6 islands. This is similar to deploying VPNs on IP networks with tunneling technologies.

The IPv6 over IPv4 tunnel connects IPv6 islands over IPv4 networks. The island connecting IPv6 islands over IPv4 networks is called IPv6 over IPv4 tunnel. To realize the IPv6 over IPv4 tunnel, the user needs to enable the IPv4/IPv6 dual stack on the routing device at the border of IPv4 and IPv6 networks.

IPv4 over IPv6

The IPv4 over IPv6 tunnel connects IPv4 islands on IPv6 networks.

During the later phase of the evolution from IPv4 networks to IPv6 networks, IPv6 networks are deployed on a large scale, which may result in IPv4 islands. Through tunneling technologies, the user can create tunnels on IPv6 networks to connect IPv4 islands. This is similar to deploying VPNs on IP networks with tunneling technologies. The tunnel connecting IPv4 islands on IPv6 networks is called the IPv4 over IPv6 tunnel.

4.9 IPv4 and IPv6 Routing

Static Routing

The USG series support that users manually configure the static route to a specific destination.

On a simple network, the static routing is sufficient to ensure normal operations of the network. The configuration and application of the static routing can improve the network performance and ensure the bandwidth for important applications.

The disadvantage of the static routing is that when a fault occurs or the topology is modified on the network, the static route cannot change automatically. In this case, the administrator must reconfigure the static routing manually.

Like the IPv4 static routing, the IPv6 static routing also requires that the administrator configure the static routing manually and is applicable to simple IPv6 networks.

The IPv6 static routing and the IPv4 static routing are different in destination addresses and next hop addresses. The IPv6 static routing adopts IPv6 addresses as next hops and destination addresses, whereas the IPv4 static routing adopts IPv4 addresses as next hops and destination addresses. In addition, only the IPv4 static routing supports VPN instances.

RIP

The USG series support the configuration of the Routing Information Protocol (RIP) dynamic routes to guide the forwarding of packets.

RIP is a simple internal gateway protocol, which is based on the distance vector algorithm. Routing information is exchanged through User Datagram Protocol (UDP) packets. Port 520 is used.

RIP uses the hop count to measure the distance (the metric value) to a destination IP address. In RIP, the hop count from the router to its directly connected network is 0. The hop count from the router to the network that can be reached through one router is 1. Every time a router is added, the hop count is added by one.

To restrict the convergence time, RIP regulates that the metric value should be an integer ranging from 0 to 15. The hop count equal to or larger than 16 is defined as infinity; that is, the destination network or host is unreachable. Due to this restriction, RIP cannot be applied to large networks.

To improve performance, RIP supports setting the interval for sending packets and the maximum number of the sent packets. To prevent the routing loop, RIP supports the split horizon and poison reverse functions.

Compared with Open Shortest Path First (OSPF) and Intermediate system to intermediate system (IS-IS), RIP is easy to be implement, configure, maintain, and manage, and thus it is still widely used in actual networking. Users can configure RIP as required to discover and generate routing information.

RIPng

RIPng, also called the next-generation RIP, is modified and extended on the basis of the original RIP-2 protocol on IPv4 networks for the application of RIP on IPv6 networks. The majority RIP concepts can apply to RIPng.

RIPng is a routing protocol based on Distance Vector (D-V). It exchanges routing information through UDP packets and adopts port 521. RIPng uses the hop count to measure the distance (the metric value or overhead) to a destination host. In RIPng, the hop count between the router and its directly connected network is 0, and the hop count between the router and the network that can be reached through one router is 1. Every time a router is added, the hop count is added by one. If the hop count is not smaller than 16, the destination network or host is identified as unreachable.

OSPF

OSPF is an internal gateway protocol based on the link status developed by Internet Engineering Task Force (IETF).

OSPF has the following features:

- Wide application scope

  It supports networks of various scales and supports a maximum of hundreds of devices.
- Fast convergence

It sends updated packets immediately after the network topology structure changes and synchronizes the updated network topology in the autonomous system (AS).

- Loop free

  It calculates routes with the shortest path tree algorithm according to the collected link status. With this algorithm, the routing loop can be prevented.

- Area division

  It allows the network of the AS to be divided into several areas for management. Routing information among divided areas is further abstracted, which reduces the occupied bandwidth.

- Equivalent route

  It supports multiple equivalent routes to the same destination IP address.

- Routing hierarchy

  The routing is classified into the intra-area routing, inter-area routing, external type 1 routing, and external type 2 routing according to the priority.

- Authentication

  It supports packet authentication based on interfaces, which ensures the security of packet transmission.

- Multicast sending

  It sends protocol packets with multicast IP addresses on certain types of links, which reduces the interference with other devices.

OSPF is applicable to large and medium-sized networks.

OSPFv3

OSPFv3, short for OSPF version 3, supports IPv6, and defined in RFC2740 (OSPF for IPv6). The majority OSPF concepts can apply to OSPFv3.

OSPFv3 and OSPFv2 are similar in the following aspects:

- The Router ID, Area ID, and LSA Link State ID are 32 bits.
- Packets of the same types: Hello packets, DD packets, LSR packets, LSU packets, and LSAck packets.
- Same neighbor discovery mechanism and adjacency forming mechanism.
- Same LSA flooding mechanism and aging mechanism.
- Same LSA types.

OSPFv3 and OSPFv2 are different in the following aspects:

- OSPFv3 is running on the links, whereas OSPFv2 is running on network segments.
- OSPFv3 runs multiple instances on one link.
- The topological relationship of OSPFv3 is independent of IPv6 addresses.
- OSPFv3 uses IPv6 link-local address to identify neighbors.
- Three LSA flooding scopes are added.

BGP

Border Gateway Protocol (BGP) is a dynamic routing protocol among AS domains. Its basic function is to automatically exchange loop-free routing information among AS domains. The topology diagram of the AS domains are created through exchanges of information about

reachable routes, which includes the attribute of the sequence consisting of AS numbers, thus removing loops and implementing the routing policy configured by the user.

Compared with the protocols running within an AS domain, such as OSPF and RIP, BGP is an Exterior Gateway Protocol (EGP); OSPF and RIP are Interior Gateway Protocols (IGPs). BGP is usually used among Internet Service Providers (ISPs).

BGP is an external routing protocol. Different from internal routing protocols such as OSPF and RIP, the focus of BGP is not to discover and compute routes, but to control the spread of routes and select the best route.

With the information about the AS path, the route loop can be prevented thoroughly.

To control the spread and selection of routes, BGP attaches the attribute information of the route.

BGP4+

BGP4+ is a dynamic routing protocol applied between Autonomous Systems (ASs). It is the extension of BGP.

Traditional BGP 4 only manages the routing information of IPv4. The applications of other network-layer protocols (such as IPv6) are restricted to a certain extent during the spreading of routing information across the AS.

To support multiple network protocols, BGP 4 is extended by the IET to BGP4+. The present standard for BGP4+ is RFC2858 (Multiprotocol Extensions for BGP-4).

To support IPv6, BGP4+ needs to reflect the information about IPv6 protocols into Network Layer Reachable Information (NLRI) and Next_Hop attributes.

Two NLRI attributes introduced into BGP4+ are:

- MP_REACH_NLRI: Multiprotocol Reachable NLR.I: It advertises reachable routes and next-hop information.
- MP_UNREACH_NLRI: Multiprotocol Unreachable NLRI. It deletes unreachable routes.

The Next_Hop attribute in BGP4+ is expressed by an IPv6 address. It can be either an IPv6 global unicast address or a next-hop link-local address.

In BGP4+, the original messaging and routing mechanisms are not changed.

IS-IS

IS-IS is a dynamic routing protocol designed by the International Standard Organization (ISO) for Connectionless Network Protocol (CLNP).

To support IP routing, the IETF extends and modifies IS-IS in RFC1195, ensuring that IS-IS can be applied to the TCP/IP and OSI environments. The extended protocol is named as Integrated IS-IS or Dual IS-IS.

IS-IS belongs to Interior Gateway Protocol (IGP) and is applied between ASs. IS-IS is a link status protocol and performs routing calculation with the Shortest Path First (SPF) algorithm. It is quite similar to OSPF.

The extended IS-IS for IPv6 is defined in the draft-ietf-isis-ipv6-05 of IETF. The draft introduces the two Type-Length-Values (TLVs) and a Network Layer Protocol Identifier (NLPID) for the extended IS-IS. RIP and OSPF have separate versions that support IPv6, namely, RIPng and OSPFv3, but IS-IS does not have the separate versions supporting IPv6.

A TLV is a variable length field in LSPs. The two new TLVs are:

- IPv6 Reachability: The type is 236 (0xEC). It illustrates the reachability of the network by defining the routing information prefix and the metric.
- IPv6 Interface Address: The type is 232 (0xE8). It is correspond to the IP interface address TLV of the IPv4, but it changes the original 32-bit IPv4 address to a 128-bit IPv6 address.

NLPID is an 8-bit field that identifies the protocol packets of the network layer. The NLPID of the IPv6 is 142 (0x8E). If an IS-IS router supports IPv6, it advertises the IPv6 routing information with the NLPID value.

IP Unicast Policy-Based Routing

IP unicast policy-based routing is a mechanism that employs user-defined policies for selecting routes. Different from the forwarding by searching the routing table only according to the destination IP addresses of IP packets, policy-based routing of the USG flexibly specifies the routing based on source IP addresses, length, user or user group and application protocol of arrival packets. This can meet the requirements of security and load balancing.The device supports both IPv4 and IPv6 protocols.

Routing Policy

The routing policy is a technology for revising routing information to change the path that network traffic passes. The technology is realized mainly through the change of routing attributes including the reachability.

When the USG series advertise or receive routing information, certain policies can be implemented to filter routing information. For example, the USG series only receive or advertise routing information that meets certain conditions. In addition, a routing protocol may need to import routing information discovered by other routing protocols. The imported routing information must meet certain conditions and users need to configure certain attributes of the imported routing information, thus making the routing information meet the requirements of this protocol.

The USG provides seven filters for routing protocols: the ACL, address prefix list, AS path filter, community attribute filter, extended community attribute filter, and router policy.

4.10 IP Multicast

IGMP

In the TCP/IP protocol suite, the Internet Group Management Protocol (IGMP) manages IPv4 multicast members. It sets up and maintains the multicast member relationships between IP hosts and adjacent multicast routers.

After IGMP is configured on the directly-connected hosts (receivers) and multicast routers, the hosts can dynamically join related multicast groups, and multicast routers can manage multicast group members on the local network.

At present, IGMP has three versions, that is, IGMPv1 (defined by the RFC 1112), IGMPv2 (defined by the RFC 2236), and IGMPv3 (defined by the RFC 3376). All IGMP versions support the Any-Source Multicast (ASM) model; IGMPv3 supports the Source-Specific

Multicast (SSM) model, while IGMPv1 and IGMPv2 can support the SSM model only through SSM mapping.

To ensure that multicast messages reach receivers, you need to connect the receivers to the IP multicast network and let the receivers join the multicast group. In this case, you can use IGMP. IGMP manages multicast group members by exchanging IGMP messages between hosts and routers. In addition, IGMP records information about adding and leaving receivers on an interface. This ensures that the multicast data can be correctly forwarded to the interface.

IGMP Snooping

IGMP snooping, short for Internet Group Management Protocol Snooping, is a multicast suppression mechanism that operates on Layer-2 devices to manage and control multicast groups.

When IGMP snooping is disabled, packets are broadcast at Layer 2. When IGMP snooping is enabled, packets are multicast to interested receivers at Layer 2.

Three advantages of applying IGMP snooping are as follows:

- Saves network bandwidths, and is convenient for independent service charging of each user host.
- Ensures independent packet forwarding on each VLAN, and improves information security.
- Responds to link failures rapidly, and enhances reliability.

PIM-DM

Protocol Independent Multicast (PIM) indicates any unicast routing protocol, such as static routing, Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Intermediate System-to-Intermediate System (IS-IS), and Border Gateway Protocol (BGP), can provide routing information for IP multicast. Multicast routing is independent of the unicast routing protocol, only through which the corresponding multicast route entries are generated.

Protocol Independent Multicast-Dense Mode (PIM-DM) is a multicast routing protocol in dense mode. It is suitable for small networks where the distribution of group members is relatively dense.

The basic principles of PIM-DM are as follows:

- PIM-DM assumes that each subnet on the network contains at least one multicast group member, and therefore floods multicast data to all the nodes on the network. Then PIM-DM prunes the branches that do not forward multicast data, reserving only the branches that contain receivers. This flood-prune process occurs periodically. Pruned branches periodically recover to the forwarding state.
- When a multicast group member appears on the node of a pruned branch, to shorten the required time for the node to recover to the forwarding status, PIM-DM proactively restores the multicast data forwarding of the branch by using the graft mechanism.

Generally, a forwarding path in dense mode is a "source tree" rooted at the source with multicast members as the branches. Since the source tree uses the shortest path from the multicast source to the receiver, it is also called the Shortest Path Tree (SPT). The interface through which a router receives multicast data is known as the upstream interface. The interface through which the router forwards the multicast data is known as the downstream interface.

PIM-SM

Protocol Independent Multicast-Sparse Mode (PIM-SM) is a multicast routing protocol in sparse mode. It is suitable for large networks where members are sparsely and widely distributed.

The basic principles of PIM-SM are as follows:

- PIM-SM assumes that all hosts do not receive multicast data, and forwards the multicast data only to the hosts that have specifically stated the requirement. The core task for PIM-SM to implement multicast forwarding is to construct and maintain the Rendezvous Point Tree (RPT). The RPT selects a router in the PIM domain as the Rendezvous Point (RP), and then multicast data is forwarded to receivers along the RPT through the RP.
- A router connected to the receiver sends a Join message to the corresponding RP in a multicast group. The Join message is sent to the RP hop by hop, and the paths that the message travels through form the branches of the RPT.
- Before the multicast source sends multicast data to a multicast group, the Designated Router (DR) at the multicast source registers and then unicasts a Register message to the RP. Upon arriving at the RP, the message triggers the establishment of the SPT. Then the multicast source sends the multicast data to the RP along the SPT. Upon arriving at the RP, the multicast data is copied and sent to the receiver along the RPT.

MSDP

Multicast Source Discovery Protocol (MSDP) is an inter-domain multicast solution developed to interconnect multiple PIM-SM domains and discover the multicast source information in other PIM-SM domains.

In basic PIM-SM, a multicast source only registers to the RP in its PIM-SM domain, and the multicast source information about each domain is isolated. Therefore, the RP only knows the multicast information about its domain, creates a Multicast Distribution Tree (MDT) in the domain, and distributes the multicast data from the multicast source to local users.

If a mechanism can transmit the multicast source information in other domains to the RP in the domain, the RP initiates the joining to other multicast sources and creates an MDT, implementing the cross-domain transmission of multicast data. In this way, group member hosts in the domain can receive the data sent from the multicast sources in other domains.

Accordingly, by selecting proper routers on the network to establish the MSDP peer relation, MSDP can connect with the RPs in each PIM-SM domains. The MSDP peers can exchange Source Active (SA) messages to share the multicast source information.

MSDP peers are connected through TCP to implement the RPF check on received SA messages.

4.11 Access Features

Ethernet

The USG series provides the express switching capability at Layer 2 through Layer-2 interfaces, facilitating Layer-2 access.

Currently, the USG adopts Ethernet interfaces as LAN interfaces, including:

- Traditional Ethernet interface: complies with the 10Base-T physical-layer standard, supports half duplex and full duplex, and works at the rate of 10 Mbit/s.
- Fast Ethernet interface: complies with the 100Base-TX physical-layer standard that is compatible with the 10Base-T physical-layer standard, supports half duplex and full duplex operations, and works at the rate of 10 Mbit/s or 100 Mbit/s. In addition, the Fast Ethernet interface supports auto-negotiation and therefore is capable of negotiating with other network devices to automatically select the best rate and duplex mode, which simplifies system configuration and management.
- Gigabit Ethernet interface: complies with the 1000Base-T physical-layer standard, supports half duplex and full duplex, and works at the rate of 1000 Mbit/s. The Gigabit Ethernet interface can work in auto-negotiation mode, helping traffic control through negotiation.

Eth-Trunk

To improve the transmission capability of links, users can bind multiple Ethernet interfaces into one Eth-Trunk interface, of which the total bandwidth is the sum of each member interface. In so doing, users can increase the bandwidth of interfaces.

The Eth-Trunk interface ensures load balancing. It assigns flows destined for the same destination to different links, avoiding traffic congestion due to the traffic transmission on only one link.

The Eth-Trunk interface improves the link availability. On the Eth-Trunk interface, if a member interface is in Down state, the traffic can be transmitted through another interface.

Null and Loopback

A loopback interface is a logical software interface. Any data packet sent to Loopback interface is considered to be sent to the USG.

The same rule of setting IP addresses is adopted for the loopback interface and common interface. Users can dynamically create and delete the loopback interface after the system is started as required.

As the loopback interface remains Up after being created and has the loopback feature, the loopback interface is usually used for improving the reliability of configurations.

A null interface is also a logical software interface. Compared with the loopback interface, the null interface is similar to the supported null device in the operating system. Any networking data packet sent to the null interface is discarded. To configure certain applications (such as the local peer in the Shared Network Area (SNA)) without affecting the configurations on the physical interface, users need to specify an IP address for the null interface and advertise the address through routing protocols.

VLAN

Users can divide VLANs on the USG as required to realize the following functions:

- Controlling the range of the broadcast domain: The broadcast packets of the LAN are restricted within a VLAN. Therefore, bandwidths are saved and the network processing capability is improved.
- Enhancing the LAN security: Because packets are isolated by the broadcast domain on the data-link layer, hosts of each VLAN cannot communicate directly. The Layer-3 packet forwarding should be carried out through network-layer devices, such as the router or Layer-3 switch.

- Creating virtual workgroups flexibly: Workgroups that crosses the physical networks can be created through VLAN.
- The mutual access of users in the same VLAN is not controlled by the access policy.
- The mutual access of users in different VLANs is controlled by the access policy.

Port Isolation

Users can add the ports to be controlled to the port isolation group to isolate the Layer-2 and Layer-3 data packets between ports in the isolation group. The port isolation function not only improves network security, but also provides users with a flexible networking plan.

MAC Address Table

The USG maintains the MAC address table to realize the express forwarding of packets. MAC address entries include the static, dynamic, and blackhole MAC address entries.

E1 and CE1

E-carrier is a digital communication system proposed by the International Telecommunication Union-Telecommunication Standardization Sector (ITU-T). It starts from E1 and applies to all regions excluding North America.

The E1/CE1 interface has the following features:

- When working in clear channel mode, also called the unframed mode, the E1/CE1 interface is without time slots and its data bandwidth is 2.048 Mbit/s. The logical features of this interface are the same as those of the synchronous serial port. The E1/CE1 interface supports network-layer protocols such as IP and link-layer protocols such as PPP and HDLC.
- When the interface works in unchannelized mode (framed mode), time slots can be bound only once and as one channel. For example, if time slot 1 and time slot 2 are bound to form a serial port with a bandwidth of 128 kbit/s, users cannot bind the interface to any other time slots. That is, no matter how many time slots are bound to the interface, users can only bind them once and form only one serial port. The logical features of this interface are the same as those of the synchronous serial port, and the interface supports link-layer protocols such as PPP and HDLC, and network-layer protocols such as IP.
- When working in channelized mode (framed mode), the interface has 32 physical time slots that are numbered from 0 to 31. Users can randomly bind the time slots as N x 64 kbit/s logical channels. Time slot 0 is used for transmitting the synchronous frame signals and cannot be bound. When using this interface, users can randomly group the 31 time slots. Then users can adopt each group of timeslots as one interface after binding. The logical features of the timeslot groups are the same as those of the synchronous serial ports. The E1/CE1 interface supports network-layer protocols such as IP and link-layer protocols such as PPP and HDLC.

Serial Port

Serial ports, as one type of the frequently used WAN interfaces, include the synchronous serial port and asynchronous serial port.

Features of the synchronous serial port:

- The synchronous serial port can work in both Data Terminal Equipment (DTE) and Data Circuit-terminal Equipment (DCE) modes. Generally, the synchronous serial port serves as the DTE to receive the clock provided by the DCE.
- A synchronous serial port can be connected with multiple types of cables, such as V.24, V.35, X.21, RS449, and RS530. The USG automatically detects the types of cables connected with the synchronous serial port, and selects the electrical feature. In common cases, the serial port does not need manual configurations.
- The synchronous serial port supports data link-layer protocols, including Peer-Peer Protocol (PPP) and High Level Data Link Control (HDLC).
- The synchronous serial port supports IP network-layer protocols.

The asynchronous serial port can work in protocol or flow mode. When connected with a modem or an ISDN Terminal Adapter (TA), the asynchronous serial port can be adopted as the dialup interface. In protocol mode, PPP can be adopted as the link-layer protocol, and IP and IPX can be adopted as network-layer protocols.

WLAN (WiFi)

A Wireless Local Area Network (WLAN) is a local area computer network that uses a wireless channel as the transmission medium. The WLAN is an important supplement and extension of a wired network, and is gradually becoming a key feature of computer networks. The WLAN is widely used in domains that require mobile data processing, or in scenarios where the physical transmission medium cannot be laid out.

As a new way of broadband access, the WLAN becomes more and more popular and develops rapidly. Meanwhile, multiple WLAN standards are defined:

- 802.11
- Bluetooth
- High Performance Radio LAN 2 (HiperLAN2)
- Home Radio Frequency (HomeRF)

802.11 is currently a common standard for constructing the WLAN because of the simple technology, stable communications quality, and comparatively large transmission bandwidths.

3G

3G is an International Telecommunication Union (ITU) specification for the third generation (analog cellular is the first generation, digital PCS such as GSM the second) of mobile communications technology. It is a technology integrating wireless communications with multimedia communications such as the Internet. The 3G technology processes multiple media forms such as images, music, and video streams, and provides a variety of information services including web browsing, teleconference, and E-commerce. In May 2000, the ITU established standards for three mainstream wireless interfaces (WCDMA, CDMA2000, and TD-SCDMA). The standards have been written into 3G technical guide document *International Mobile Telecommunications 2000 (IMT-2000)*.

Multiple types of 3G data cards can be inserted into the USG, and LAN users can access the network from the uplink through the 3G data cards. Through different 3G data cards, the USG series supports WCDMA, CDMA2000, and TD-SCDMA.

PPP

PPP is a link-layer protocol that bears the network-layer packets on the point-to-point link. It provides the authentication function and supports synchronization and asynchronization.

PPP defines a set of protocols, including:

Link Control Protocol (LCP): is used for establishing, tearing down, and monitoring data links.

Network Control Protocol (NCP): is used for negotiating the format and type of data packets transmitted on data links.

Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP): are used for authenticate network security.

MP

To increase bandwidths, Multilink Protocol (MP) binds multiple PPP links. MPs can be applied to the interfaces (such as channelized serial interfaces or low-speed POS interfaces) that support PPP.

MP allows the fragmentation of packets, and the fragments are sent to the same destination through multiple PPP links of MP.

MP negotiation includes the processes of LCP negotiation and NCP negotiation.

- LCP negotiation: Both ends perform LCP negotiation first. In addition to the negotiation of common LCP parameters, LCP negotiation checks whether the peer interface works in MP mode. If the working modes of two ends are inconsistent, LCP negotiation fails.
- NCP negotiation: NCP negotiation is performed based on the NCP parameters (such as the IP address) of the MP-Group interface, and the parameters specified on the physical interface do not take effect.

After NCP negotiation is passed, the MP link can be established.

HDLC

The High-level Data Link Control (HDLC) protocol transparently transmits any type of bit flow. The data is not required to be a character set.

The protocols in the standard HDLC protocol family are executed on the synchronous serial line, such as the Digital Data Network (DDN).

Both the address and control fields of HDLC are eight bits to realize the control information of HDLC and identify whether it is data.

MSTP

Multiple Spanning Tree Protocol (MSTP) is compatible with Spanning Tree Protocol (Spanning Tree Protocol) and Rapid Spanning Tree Protocol (RSTP) to make up the defects of STP and RSTP. STP selectively blocks redundant links on Layer-2 networks, and prunes the network as a tree status, eliminating loops. It also provides the link backup function. MSTP supports fast convergence and enables the forwarding of the traffic of different VLANs along their paths, providing the sound load balancing mechanism for redundant links.

PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) uses the Ethernet to form a network of a large number of hosts and connects the network to the Internet through a remote access device.

After the configuration of PPPoE, a PPP session with the remote device can be created to implement access control and accounting.

The USG serves as a PPPoE server, to which the PPPoE clients of various types connect in the Ethernet environment.

The USG can be used as a PPPoE client device to perform the dialing function.

ADSL

ADSL is a technology that provides high bandwidth access. It is mainly applied to asymmetric rate transmission. ADSL uses current telephone lines to transmit high speed data and provides users with multiple services such as the high speed Internet access, Video on Demand (VOD), and video telephony.

ADSL2+ is a new generation ADSL standard passed on the ITU conference in January 2003. It is an extended ADSL standard on the basis of ADSL2.

The ADSL2+ interface module can be inserted into the USG for supporting the ADSL2+ feature.

G.SHDSL

The SHDSL, also known as G.SHDSL, is an international standard for symmetrical DSL developed by the ITU-T (in G.991.2). The SHDSL transmits bidirectional symmetrical broadband data over a single twisted pair. SHDSL is a symmetrical transmission technology with the longest distance among all DSL technologies.

The G.SHDSL interface module can be inserted into the MIC slot of the USG for supporting the SHDSL feature.

4.12 System Management

Information Center

USG can be managed by centralized management platforms. The information center receives and processes log, debugging, and alarm information, helping network administrators and developers monitor network running status and diagnose network faults.

SNMP

At present, the Simple Network Management Protocol (SNMP) is an industry standard that is widely used in network management.

SNMP aims to ensure the transmission of management information between two nodes. In this way, the administrator can search for and modify information, troubleshoot and diagnose faults, and determine the capacity, so that reports are generated on any node.

SNMP adopts the polling mechanism, provides a basic function set, and applies to small, high-speed, and low-price networks. SNMP is widely supported by products because it only requires the connectionless UDP at the transport layer.

The device supports SNMPv3, and is compatible with SNMPv1 and SNMPv2c.

LLDP

The Link Layer Discovery Protocol (LLDP) is a Layer 2 Discovery protocol defined in IEEE 802.1AB. Using the LLDP, the Network Management System (NMS) can rapidly obtain the Layer 2 network topology and changes in topology when the network scales expand.

With LLDP, a standard means of link layer discovery, the information such as main capabilities, management addresses, and device and interface identifiers of the local end forms different Type/Length/Values (TLVs), and is encapsulated into Link Layer Discovery Protocol Data Units (LLDPDUs). Then these LLDPDUs are advertised to the directly-connected neighbors and saved on the neighbor in the form of the standard Management Information Base (MIB), facilitating NMS query and link communication check.

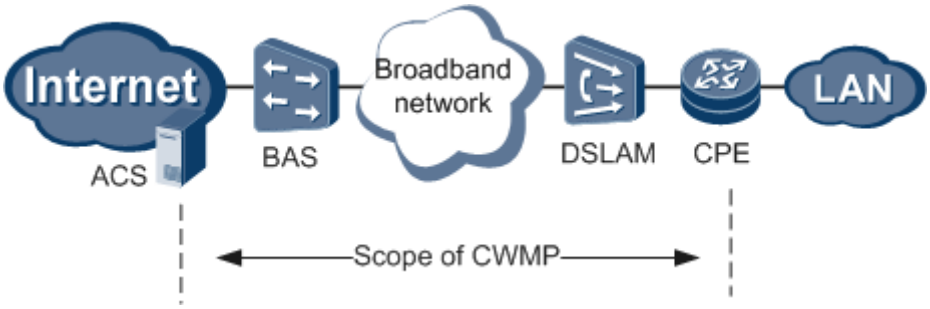
CWMP (TR-069)

With the CPE WAN Management Protocol (CWMP), Customer Premises Equipment (CPE) can be managed in a centralized way through the Auto-Configuration Server (ACS) in terms of configuration management, version management, and remote monitoring and diagnoses.

CWMP is one of the technical standards initiated and developed by the Digital Subscriber's Line (DSL) forum. CWMP provides the general frameworks, information standards, management methods, and data models for the management configuration of the home network devices of the next generation network. CWMP is mainly applied to DSL access networks. On DSL access networks, lots of devices are dispersedly deployed at the user side, and hence are hard to manage and maintain. Accordingly, with CWMP, users can remotely and globally manage CPE through the ACS to reduce maintenance costs and improve the efficiency of solving problems.

The following figure shows the typical networking diagram of CWMP. Generally, CPE (such as the gateway and set-box) is of various types and dispersedly deployed. Therefore, it is inconvenient for the O&M personnel of carriers to change configurations or troubleshoot faults onsite. CWMP solves this problem. CWMP, however, provides the general frameworks and protocols for managing and configuring user terminals, thus realizing the remote and centralized management over CPE at the network side. Through CWMP, the ACS completes the configuration, diagnoses, and upgrade of devices at the user side, which greatly reduces maintenance costs.

Figure 4-5 Typical application of CWMP (TR-069)



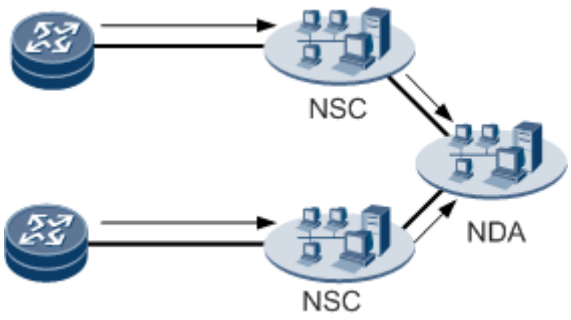
NetStream

NetStream collects statistics on network traffic, and periodically sends statistics to the NetStream Collector (NSC). The statistics can be used for charging, and network management and planning.

With the increase of network services and applications, users have higher requirements for traffic statistics and analysis. NetStream meets the requirements. It provides network administrators with the method of accessing the details on their networks. Output NetStream data can be applied to multiple aspects, including network management and planning, enterprise accounting, department-based charging, ISP compilation billing, data storage, and commercially-oriented data collection.

On networks, the IP network is connectionless. Therefore, the communications between different types of services are implemented through a group of IP packets sent from one terminal to another. Actually, these IP packets form the data flows of a network service. Most data flows are temporary, intermittent, and bidirectional. NetStream mainly identifies different flows based on the septuple form constructed by the destination and source IP addresses, destination and source port numbers, protocol numbers, ToS, and input and output interfaces, and collects data statistics on these flows. The routing device is responsible for collecting flow statistics and then output the collected statistics to a NetStream Collector (NSC). After collecting and storing the statistics from the NDE, the NSC filters and aggregates the flows and output them to a NetStream data analyzer (NDA). The NDA further aggregates the statistics, orders them, and displays various statistics in the format of diagrams.By analyzing the statistics output from the NDA, you can perform network accounting, network planning, network monitoring, application monitoring, and fault location and diagnosis.

Figure 4-6 Typical application of NetStream



The device sends the obtained statistics on flows to the NSC, and the NSC processes and sends the statistics to the NDA. Then the NDA analyzes and further processes the statistics.

NTP

Network Time Protocol (NTP) is to synchronize the time of all devices that have clocks, so that the time consistency is ensured on the entire network and devices provide various applications based on the unified time. The system running NTP can proactively synchronize other systems, be synchronized by other systems, or exchange NTP packets with other systems for mutual synchronization.

NTP adopts UDP and port 123 for traffic transmission.

NQA

The Network Quality Analysis (NQA) function tests the performance of various protocols running on networks. In addition, the NQA is an effective tool for fault diagnoses and location.

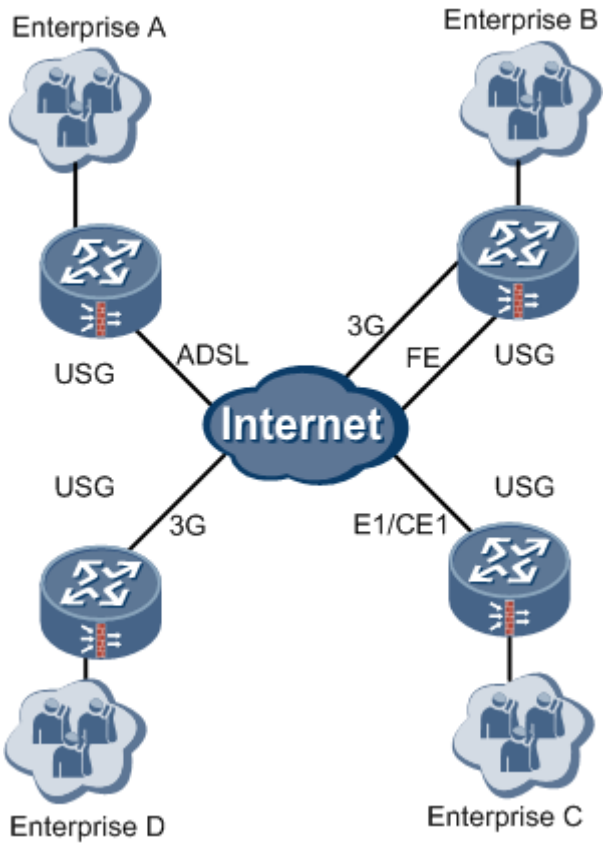
It expands and enhances the ping function, detects whether the TCP, UDP, DHCP, FTP, HTTP, and SNMP services are enabled, and tests the response time of various services.

5 Application Scenario

About This Chapter

5.1 Comprehensive Access Solution

Figure 5-1 Multiple Modes of Accessing the Internet

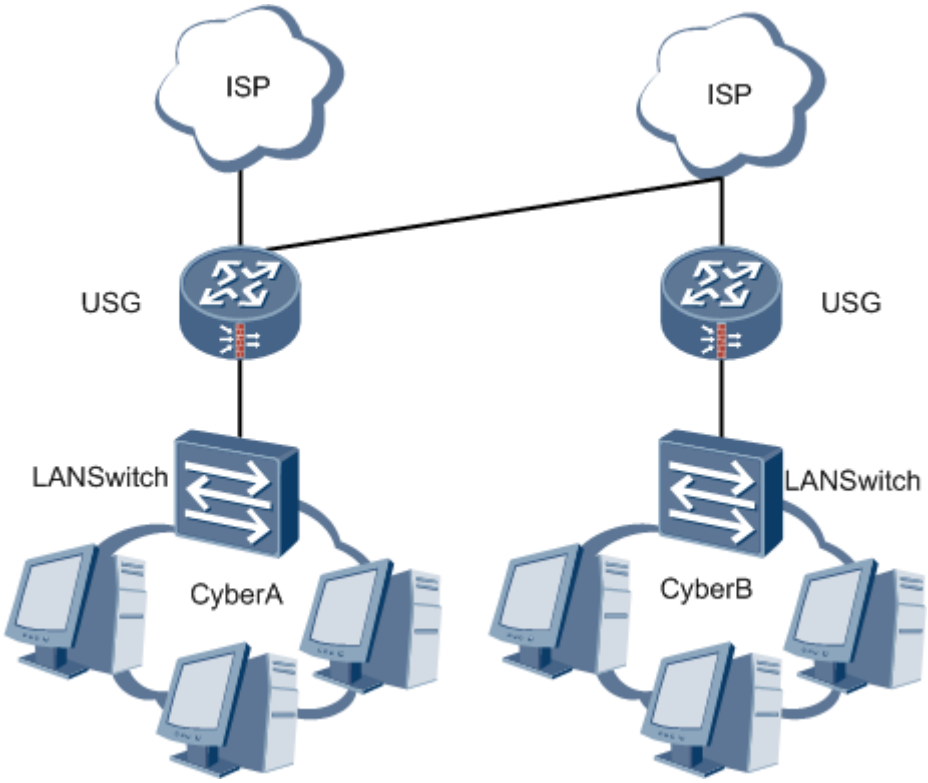


Users can select the access modes including E1/CE1, FE, GE, 3G, WLAN, ADSL2+, or G.SHDSL according to the networking environment provided by the carrier. The USG provides dual uplinks, ensuring the reliability of Internet services.

- Routing, security, switching, VPN, and wireless functions, ensuring the secure, fast, and reliable forwarding of packets
- Attack defense, defending various attacks from external and internal networks
- Congestion management and CAR, providing sufficient bandwidths for users' access to the Internet
- NAT

5.2 Egress Gateways for Cyber Bars

Figure 5-2 Egress gateways for cyber bars

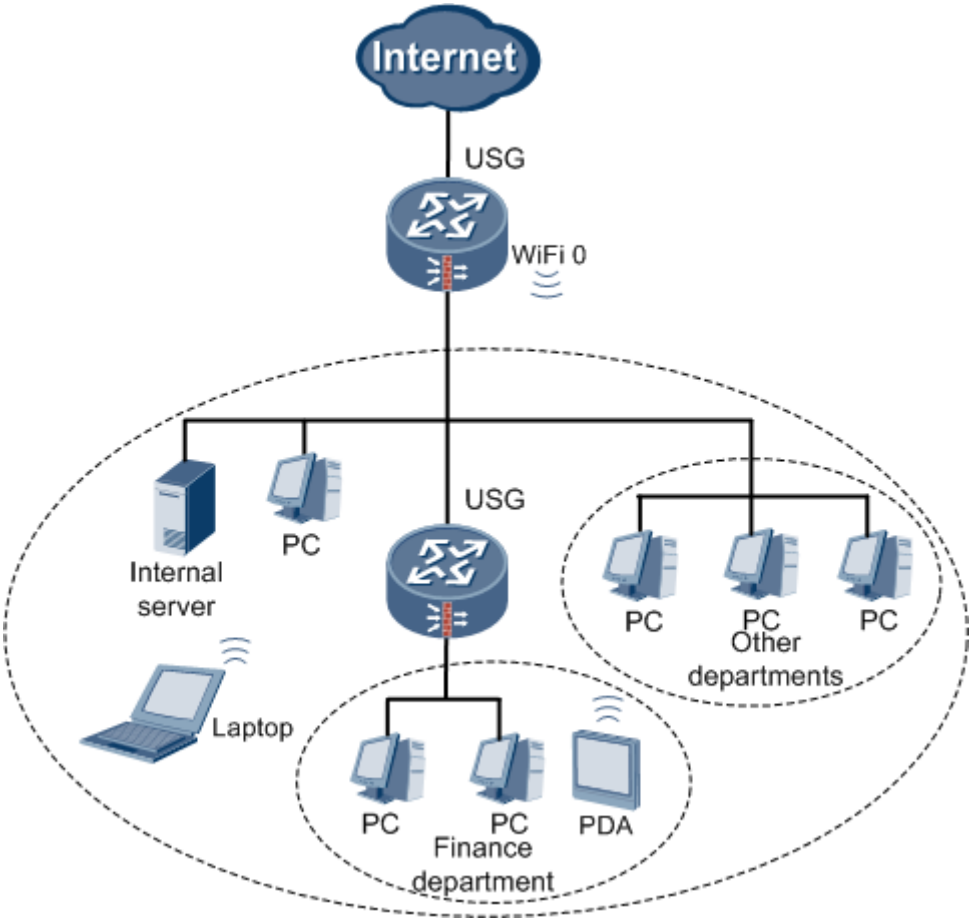


The USG serves as the egress gateway for large cyber bars for users to access the Internet.

- Routing function, facilitating the fast and precise forwarding of packets.
- Attack defense function, defending against various attacks from external and internal networks.
- Congestion management and CAR traffic control, ensuring sufficient bandwidths for users' access to the Internet.
- Dual uplinks, ensuring service reliability for online users.
- Line stability of Internet access with heavy traffic.

5.3 Protecting Internal LANs

Figure 5-3 Protecting Internal LANs

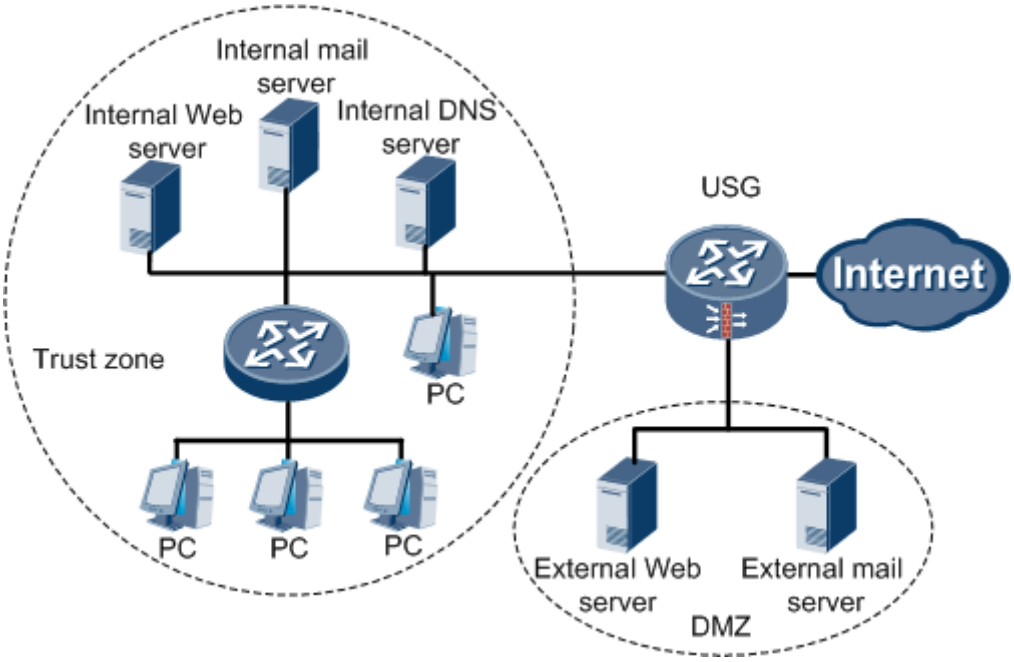


The USG can be deployed at either the interface between enterprise intranets and extranets, or key positions of enterprise LANs, securing important resources.

As shown in Figure 5-3, the enterprise LAN is connected with the Internet through the USG to restrict Internet users' access to enterprise LANs. If enterprise LAN users need to access Internet resources,the users can access the extranet through Network Address Translation (NAT) after passing the authentication.Key departments (such as the finance department) have their own LANs protected by the USG to prevent unauthorized internal users from accessing key resources.

5.4 Opening Intranet Servers Securely

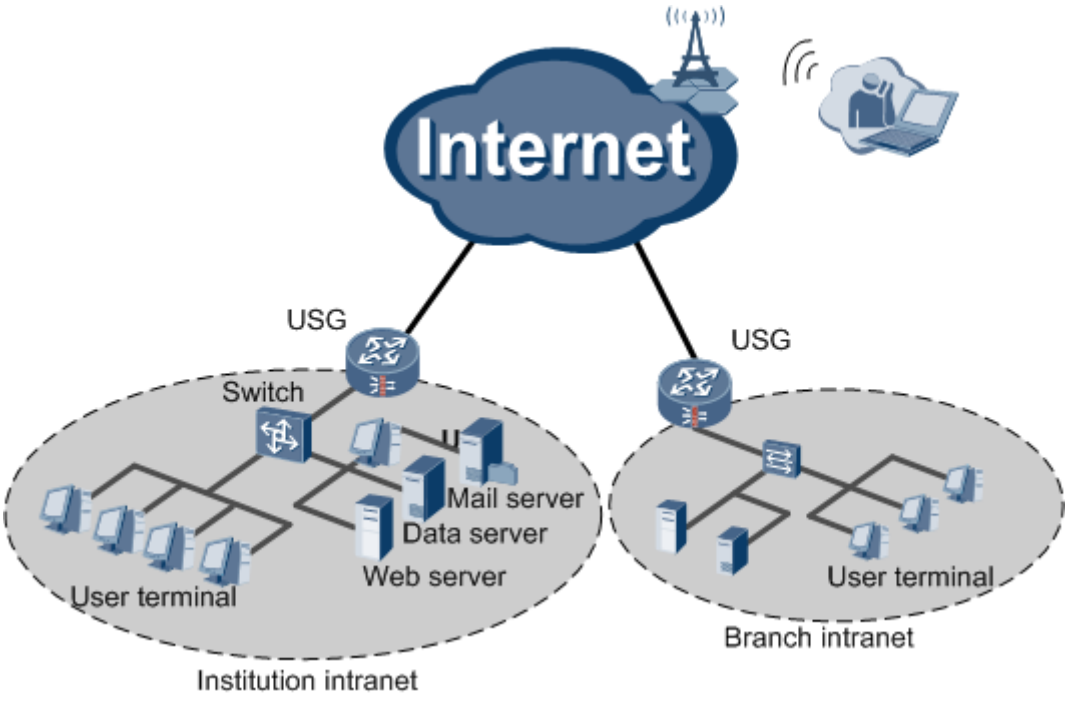
Figure 5-4 Opening intranet servers securely



If the data center, Internet Service Providers (ISPs), communities, schools, and governments need to provide services (such as Web and email), packets can be filtered through the USG. For example, only packets to certain ports opened to external users are allowed through. The USG detects and defends against various attacks.

5.5 Intranet User Management

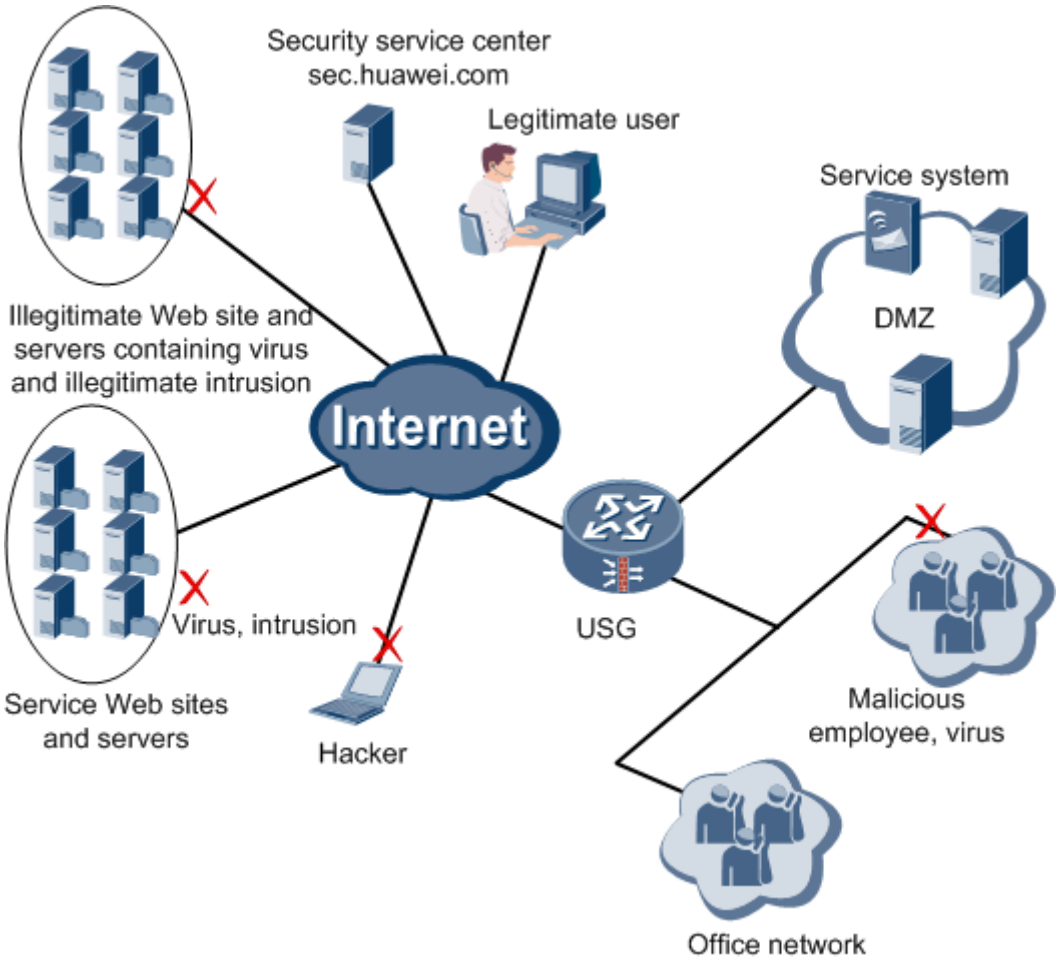
Figure 5-5 Intranet user management



- Authorize the network access of intranet users using the Network User Management.
- Reference the control policies and traffic control policies using policy unification to identify various applications with precision; configure traffic control based on individual or multiple IP addresses; configure maximum bandwidth and minimum available bandwidth to minimize the bandwidth consumed by non-service applications and provide service applications with sufficient bandwidth meeting the bandwidth requirement of service applications and utilizing the limited bandwidth.

5.6 Security Protection for Enterprises and Government Agencies

Figure 5-6 Security protection

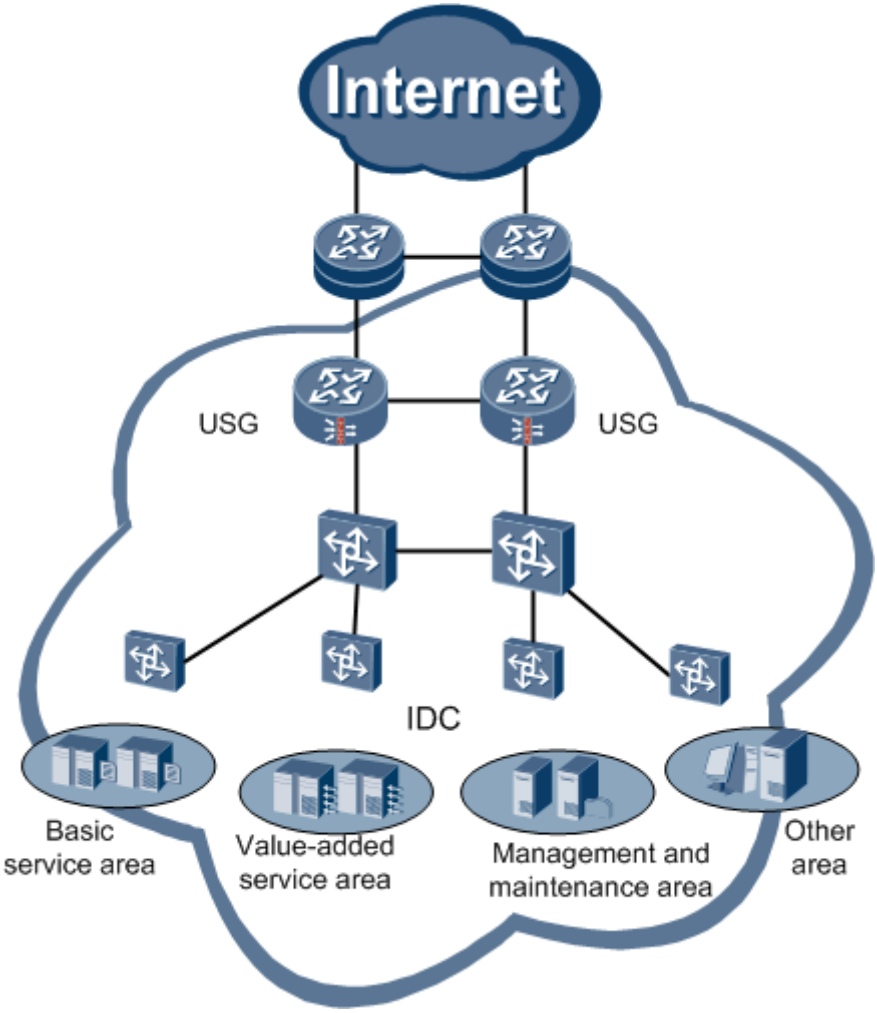


- Security protection for mission-critical applications on the intranet
  - Attack defense
  - IPS
  - AV
  - Email filtering
- Network access
  - Supports NAT to allow internal users to access the Internet and supports NAT server to allow external users to access the internal mail and web servers on the intranet.
  - Supports IPSec, L2TP, and SSL VPN for employees at branches and on business trips to securely access the resources at the headquarters.
- Online behavior control
  - Supports P2P traffic limiting
  - Supports IM blocking

- Supports URL filtering

5.7 Security Protection for IDCs

Figure 5-7 IDC security protection networking diagram



The two USGs are deployed at the egress of the IDC to deliver basic routing, firewall, IPS, AV, and URL filtering functions.

IPS performs in-depth inspection to detect application-layer attacks and blocks the attack traffic.

AV scans the files transmitted through HTTP, SMTP, and POP3 for virus-infected files and processes the files according to configured policies.

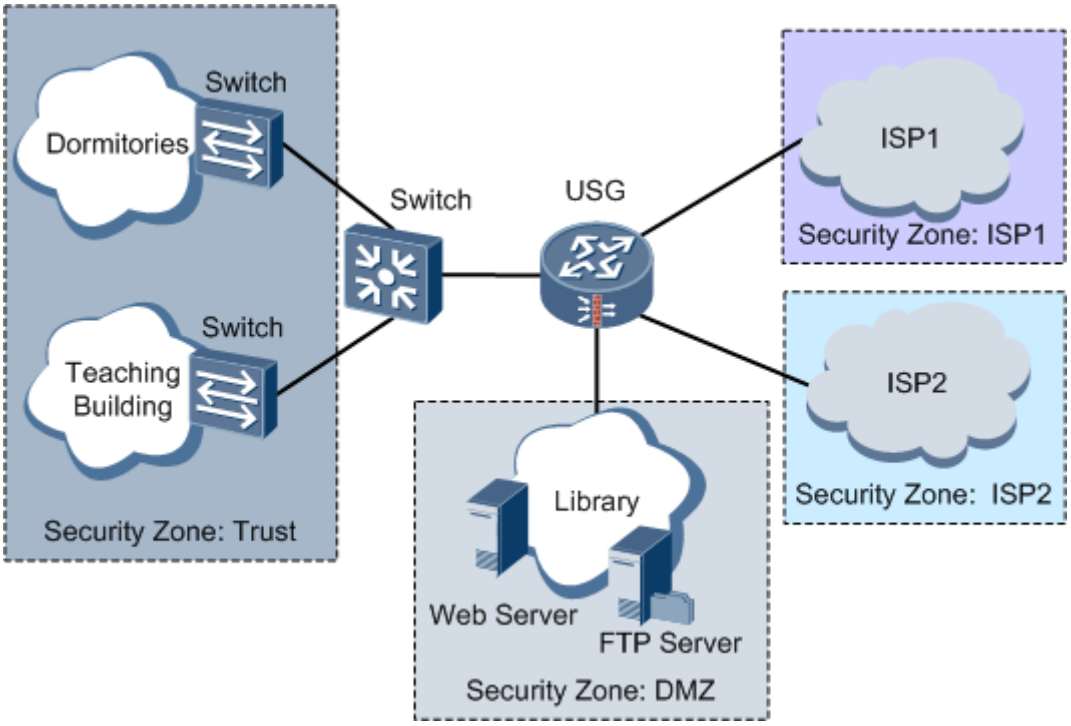
URL filtering controls online behaviors, restricts applications that may compromise the internal security and legitimate applications, and monitors the applications running on terminals of internal users for future audit.

The security service center on the Internet enables the online update of the IPS signature database and virus database on the USG to keep the databases up-to-date to prevent the latest intrusions and viruses.

5.8 Security Protection for Campus Networks

Figure 5-8 shows the application of the USG on a campus network.

Figure 5-8 Campus network security protection networking diagram



- To enable campus users to access the Internet using the limited public IP addresses, NAPT is required to translate a large number of private IP addresses into a small number of public IP addresses.

  Because the campus network is connected to two ISPs, the private IP addresses must be translated into the respective public IP addresses provided by the two ISPs. To configure NAPT, you must create two security zones, namely, ISP1 zone and ISP2 zone, and the priorities of these two security zones must be lower than that of the DMZ. Then, configure NAT outbound between the Trust zone and the ISP1 zone and between the Trust zone and the ISP2 zone.
- To ensure that packets can be forwarded to both ISPs, you must collect the routing information of both ISP networks and configure static routes to the two ISP networks. The traffic to ISP1 is forwarded through the interface connected to ISP1 whereas that to ISP2 is forwarded through the interface connected to ISP2.

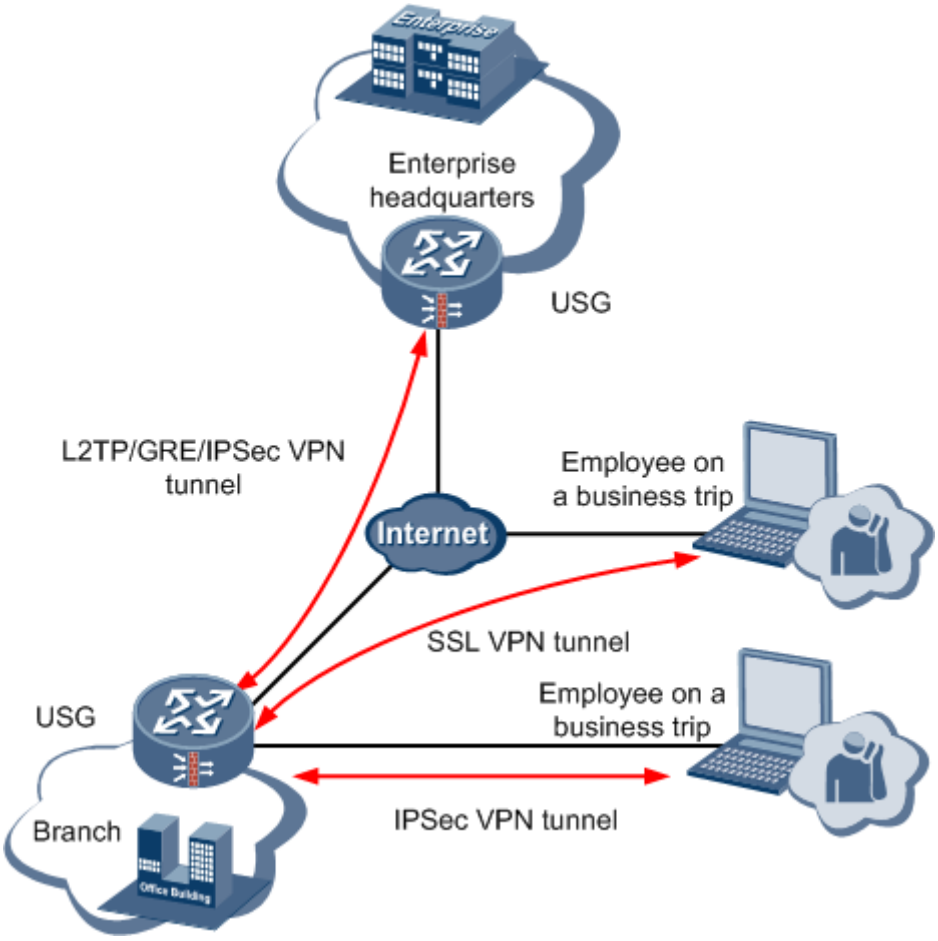
  To improve link availability and avoid service interruption, you must configure two default routes, one to each ISP network. When the destination IP addresses do not match any static routes, packets can be forwarded to the next hop through the default routes.

- The servers at the library are on the private network. To enable the servers to provide services for external users, you must configure NAT server to translate the private IP addresses of the internal servers to the public IP addresses on the ISP1 and ISP2 networks.
- P2P traffic must be restricted to avoid the waste of the limited bandwidth resources and the impact on other applications.
- The attack defense can be enabled on the USG to protect the security of the campus network.

5.9 VPN Applications

The VPN technologies allow geographically dispersed branches and employees on business trips to be securely connected to the headquarters anytime, anywhere, and on any device.

Figure 5-9 VPN access



As shown in Figure 5-9, the headquarters is connected to the Internet through the USG. It is required that servers at the headquarters are accessible to branches and employees on business trips. Branches are also connected to the Internet through the USG and must be accessible to external users. Branch users can access the servers or LAN hosts at the headquarters, and

employees on business trips can access the resources on the intranet through IPSec VPN or SSL VPN.

The L2TP VPN, GRE VPN, or IPSec VPN connects the headquarters, branches, and the employees on business trips into one intranet. Employees on business trips can access the intranet through IPSec or SSL VPN tunnels after being authenticated by the server.

6 Operation and Maintenance

About This Chapter

6.1 Multiple Configuration and Management Modes

Console

You can connect a configuration terminal to the console port of the device to configure and maintain it.

Telnet

If the IP connectivity is available between the configuration terminal and the device, you can telnet to the device to configure and maintain it from the configuration terminal.

SSH

The device supports Secure Shell (SSH), which provides authentication and encryption functions to secure communications against attacks such as IP address spoofing and password interception.

Web

You can configure the device through the sWeb platform.

You can configure and manage the device on an user-friendly GUI-based Web interface through HTTP or HTTPS.

On the Web interface, you can configure the statistics parameters and functions such as security zones, ACLs, NAT, ASPF, attack defense, blacklist, VLAN, QoS, IPS, application control, VPN, policy-based routing, and load balancing.

SNMP-based Device Management

The device supports SNMP (v1/v2c/v3) and the client/server structure, and can be managed by an NMS.

Upgrade Through the USB Disk

The device supports upgrade through the USB disk automatically and manually, featuring convenient upgrade and configuration.

One-Button Recovery

The device supports one-button recovery. Press the Reset button on the panel, and the device is restored to default configurations.

6.2 Maintenance Functions

- Remote packet capture

  The remote packet capture function caches and sends the packets passing through the USG to a remote host for analysis.
- Packet loss statistics collection

  The USG provides packet loss statistics for analysis.
- Multiple update methods

  The DPI rule base supports automatic online update, manual online update, and local update.

  The IPS signature database and virus database support automatic online update, manual online update, local update, and version rollback.
- Debugging function

  The USG supports debugging while running to log the information about key events, packet processing, packet parsing, and status switchover, facilitating debugging and network planning. You can enable or disable the debugging function for a specific service (such as a routing protocol) or on a specific interface (such as a specified interface running the protocol) through the console. The trace function of the USG can log key events such as task switchover, interruption, queue reading/writing, and system anomalies. When the system restarts from a fault, the trace information can facilitate future troubleshooting. You can enable or disable the trace function by using console commands.
- Configuration file backup for disaster recovery

  You can specify a backup configuration file as the startup configuration file for disaster recovery when the original startup file is damaged or lost.
- Web interface diagnosis

  The sWeb provides diagnosis functions including IPSec negotiation diagnosis, 3G access diagnosis, ADSL access diagnosis, Web page open failure diagnosis. The diagnosis functions greatly facilitate the fault locating and troubleshooting.

6.3 Enhanced Log Functions

- Two types of logs

  The USG supports text syslogs, and can create information table based on flow status and generate fast binary logs for the heavy traffic passing through the USG.

- Various logs

  The USG provides logs about traffic monitoring, blacklist, attack defense, address binding, Web access, packet filtering, AV, IPS, URL filtering, and NAT/ASPF.

- Interworking with the eLog

  The eLog is a device log management system developed by Huawei. The eLog collects the logs from devices to provide visibility into the running status of network and security devices, track the behaviors of users, and identify and eliminate threats.

  The USG can collaborate with the eLog to store the massive logs for convenient log query, facilitating the locating of network faults and historical device running information.

- Log servers for disaster recovery

  The USG can send logs to a maximum of 16 log servers. The USG can poll the log servers and send logs to proper servers or send logs to all servers concurrently.

6.4 Security

Data System Security

The system takes the following measures to ensure data security:

- Backup and recovery policy

  Save the data (the system software, configuration file, log file, and database data) at a certain time spot to other storage devices. When the system becomes faulty, import the backup data to the system to restore the normal operation of the system.

- Configuration file backup for disaster recovery

  You can specify a configuration file for disaster recovery and designate the file as the startup configuration file. In so doing, when the configuration file in use failed to be recovered, you can still use the initial services normally.

Operation and Maintenance Security

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

- Administrator permission control.

  The USG 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 USG supports the isolation of the in-band management plane and provides a dedicated management port instead of using the service ports for management.

If users connect to the USG 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.

The communication between the USG and the third-party NMS is implemented using security protocols. You can enable the services of the security protocols, such as HTTPS. You can disable the services of insecure protocols, such as HTTP and Telnet.

- Security logging

  The system can log important operations such as login and logout for future audit.

- Protection mechanism for the sensitive user information

  The system authenticates users through password and identity authentication, and protects the sensitive user information using the advanced encryption algorithm. Every user is allocated with a password for the verification before the system provides services for the user, protecting the security of user information. When the administrator logs in to the device, the system forces the administrator to change the default password to enhance security management.

  You can configure audit-level users to view the sensitive logs on UTM features, avoiding data leaks.

- Anti-brute-force mechanism

  Some unauthorized users attempts to hack into the system by conjecturing the administrator's user name and password. The USG supports the maximum number of login attempts. Once the number of login attempts exceed 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.

7 Technical Specifications

About This Chapter

7.1 System Specifications

Table 7-1 Overall system specifications

Item	USG2110-X	USG2100	USG2200	USG5100	USG5500
Dimensions (H x W x D)	260 mm x 170 mm x 43.6 mm	420mm×255 mm×43.6mm	43.6 mm x 442 mm x 414 mm	• USG5120: 86.1 mm x 442 mm x 414 mm • USG5150:130.5 mm x 442 mm x 414 mm	• USG5520S/5530S: 43.6 mm x 442 mm x 560 mm • USG5530/5550/5560: 130.5 mm x 442 mm x 414.1 mm
Weight	≤ 2 kg	5kg (net weight), ≤ 8kg (in full configuration)	Base chassis: 5.4 kg; fully configured chassis: 8 kg	• USG5120: Base chassis: 6.5 kg; fully configured chassis:	• USG5520S/5530S: Base chassis: 8.24 kg; fully configured chassis:

Item	USG2110-X	USG2100	USG2200	USG5100	USG5500
				13.5 kg • USG5150: Base chassis: 8.3 kg; fully configured chassis: 17.5 kg	8.9 kg • USG5530: Base chassis: 15.8 kg; fully configured chassis: 17.9 kg • USG5550: Base chassis: 16.5 kg; fully configured chassis: 18.3 kg • USG5560: Base chassis: 16.6 kg; fully configured chassis: 18.4 kg
CPU	333 MHz	333MHz	Multi-core MIPS processor; frequency: 750 MHz	Multi-core MIPS processor; frequency: 1 GHz	Multi-core MIPS processor; frequency: 950 MHz
Memory	512 MB	512 MB	2 GB	2 GB	4 GB
NVRAM	-	-	512 KB (in the Flash memory)	256 KB	512 KB
Flash memory	64 MB	32 MB	64 MB	64 MB	64 MB
CF card	-	-	Not supported	Not supported	2GB
microSD card	-	2 GB or 4 GB microSD card for standard configuration	2 GB or 4 GB microSD card for standard configuration	2 GB or 4 GB microSD card for standard configuration	Not supported
Rated input voltage	AC: 100 V to 240 V (50/60 Hz)	AC: 100V to 240V (50/60Hz)	AC: 100 V to 240 V (50 Hz/60 Hz)	AC: 100 V to 240 V (50 Hz/60 Hz)	AC: 100 V to 240 V (50 Hz/60 Hz)

Item	USG2110-X	USG2100	USG2200	USG5100	USG5500
					DC: -48 V to -60 V
Maximum power	18 W	AC: 54W	100 W	• USG5120: 210 W • USG5150: 300 W	• USG5520S/5530S: 150 W • USG5530/5550/5560: 300 W

NOTE

- The Flash memory stores the startup and configuration files of the device. It has a small capacity and is fixed in the device.
- microSD cards and CF cards have relatively large capacity, and are used for storing startup and configuration files. The microSD cards and CF cards can be replaced with one of larger capacity.

7.2 Environment Requirements

Table 7-2 Environment requirements

Item	Description
Altitude	≤ 2000 m (Long-term operating temperature: 0°C to 45°C)
Atmospheric pressure	70 kPa to 106 kPa
Operating temperature	Long term: 0°C to 45°C Short term: –5 °C to +55 °C
Storage temperature	–40 °C to +70 °C
Relative humidity (operating and storage)	Long term: 10% RH to 90% RH, non-condensing Short term: 5% RH to 95% RH, non-condensing

7.3 Standard and Protocol Compliance

Table 7-3 ETS standards

Standard	Description
ETS 300 019-2-2	Equipment Engineering; Environmental conditions and environmental tests for telecommunications equipment. part2-2: specification of environmental tests transportation

Standard	Description
ETS 300 119-3	European telecommunication standard for equipment practice Part 3: Engineering requirements for miscellaneous racks and cabinets
EN 300 386 Version 1.2.1	Electromagnetic compatibility and Radio spectrum Matters (ERM); Telecommunication network equipment; ElectroMagnetic Compatibility (EMC) requirements

Table 7-4 IEC standards

Standard	Description
IEC 61000	Electromagnetic compatibility (EMC)
IEC 61000-4-2	Electromagnetic compatibility (EMC) - Part 4: Testing and measuring techniques - Section 2: Electrostatic discharge immunity test - Basic EMC publication
IEC 61000-4-3	Electromagnetic compatibility (EMC) - Part 4-3: Testing and measurement techniques; Radiated, radio-frequency, electromagnetic field immunity test
IEC 61000-4-4	Electromagnetic compatibility (EMC) - Part 4: Testing and measuring techniques - Section 4: Electrical fast transient/burst immunity test - Basic EMC publication
IEC 61000-4-5	Electromagnetic compatibility (EMC) - Part 4: Testing and measurement techniques - Section 5: Surge immunity test
IEC 61000-4-6	Electromagnetic compatibility (EMC) - Part 4: Testing and measurement techniques - Section 6: Immunity to conducted disturbances, induced by radio-frequency fields
IEC 61000-3-2	Electromagnetic compatibility (EMC) - Part 3-2: Limits; Limits for harmonic current emissions (equipment input current <kleiner =>16 A per phase)
IEC 61000-3-3	Electromagnetic compatibility (EMC) - Part 3: Limits; section 3: Limitation of voltage fluctuations and flicker in low-voltage supply systems for equipment with rated current <kleiner =>16 A
IEC 62151	Safety of equipment electrically connected to a telecommunication network

Table 7-5 ISO standards

Standard	Description
ISO/IEC 11801	Information technology - Generic cabling for customer premises
ISO/IEC 15802-2	Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Common specifications - Part 2: LAN/MAN management

Table 7-6 CISPR standards

Standard	Description
CISPR 22	Information technology equipment - Radio disturbance characteristics - Limits and methods of measurement

Table 7-7 ITU-T standards

Standard	Description
I.430	[I.430] Recommendation I.430 (11/95) - Basic user-network interface - Layer 1 specification
I.431	[I.431] Recommendation I.431 (03/93) - Primary rate user-network interface - Layer 1 specification

Table 7-8 IEEE standards

Standard	Description
IEEE802.3	Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specification
IEEE802.3u	Media Access Control (MAC) parameters, physical Layer, medium attachment units, and repeater for 100 Mb/s operation, type 100Base-T
IEEE802.1D	Media Access Control (MAC) Bridges
IEEE802.3af	DTE Power via MDI

Table 7-9 National standards of P.R. China

Standard	Description
YDN028-1997	SDH optical fiber system and device linear MSP — linear multiplex section, self-healing ring, and other types of structures
YDN 062-1997	Fault detection and location procedure for PDH channel, section, and transmission system, and SDH channel and multiplex section
GB/T 13543-92	Environmental test methods for digital communication equipment
GB 2421-89	Environmental testing for electric and electronic products-General requirements
GB 2423.1-89	Basic environmental testing procedures for electric and electronic products Tests A: Cold
GB 2423.2-89	Basic environmental testing procedures for electric and electronic

Standard	Description
	products Tests B: Dry heat
GB/T 2423.3-93	Basic environmental testing procedures for electric and electronic products Test Ca: Damp heat, steady state
GB/T 2423.5-1995	Environmental testing for electric and electronic products-Part 2: Test methods Test Ea and guidance: Shock
GB/T 2423.6-1995	Environmental testing for electric and electronic products-Part 2: Test methods Test Eb and guidance: Bump
GB 2423.9-89	Environmental testing for electric and electronic products Part 2: Test methods Test Cb: Damp heat, steady state, primarily for equipment
GB/T 2423.10-1995	Environmental testing for electric and electronic products-Part 2: Test methods Test Fc and guidance: Vibration (Sinusoidal)
GB 2423.22-87	Basic environmental testing procedures for electric and electronic products — Test N: change of temperature
GB 2423.43-1995	Environmental testing for electric and electronic products — Part 2: Test methods — Mounting of components, equipment and other articles for dynamic tests including shock (Ea), bump (Eb), vibration (Fc and Fd) and steady-state acceleration (Ca) and guidance
GB2424.1-89	Basic environmental testing procedures for electric and electronic products — Guidance for high temperature and low temperature tests
GB/T2424.2-93	Basic environmental testing procedures for electric and electronic products — Guidance for damp heat tests
GB2424.13-81	Electric and electronic products — Basic environmental test regulations for electricians — Guidelines for temperature variation tests
SJ2170-82-SJ2175-82	Basic test method for common electronic product transport package
SJ 3213-89-SJ 3215-89	Basic test method for common electronic product transport package
SJ/Z 3216-89	Electronic product protection, package, and packing level
GB 3873-83	General Technical Conditions for Communication Equipment Product Package
GB/T 4857.1-92	Marking methods for package, transport package tests
GB/T 14013-92	Mobile communication device — transport package
GB191-1990	Packaging-Pictorial markings for handling of goods
GB6388-1986	Transport package shipping mark
GB/T 13426-1992	Reliability Requirements and Test Methods for Digital Communication Equipment

8 Ordering Guide

About This Chapter

8.1 Chassis Ordering

Table 8-1 shows the basic specifications of the USG5500.

Table 8-1 Available models of the USG5500

Device Model	CPU	Memory	Flash memory	CF card	MIC/DMIC slot	FIC/DFIC slot
USG5520S	950 MHz	4 GB	64 MB	2 GB	0/0	2/1
USG5530S	950 MHz	4 GB	64 MB	2 GB	0/0	2/1
USG5530	950 MHz	4 GB	64 MB	2 GB	2/1	6/4
USG5550	950 MHz	4 GB	64 MB	2 GB	2/1	5/3
USG5560	950 MHz	4 GB	64 MB	2 GB	2/1	5/3

Table 8-2 shows the USG2110-X/2100/2200/5100 models classified based on the CPU frequency, memory capacity, and Flash memory capacity, and the number of MIC and FIC slots.

Table 8-2 Available models of the USG2110-X/2100/2200/5100

Model	CPU	Memory	Flash memory	microSD card	MIC/DMIC slot	FIC/DFIC slot
USG2110-X	333 MHz	512 MB	64 MB	-	0/0	0/0
USG2160/USG2160W	333 MHz	512 MB	32 MB	2 GB/4 GB	2/1	0/0
USG2200	750 MHz	2 GB	64 MB	2 GB/4 GB	4/2	2/1
USG5120	1 GHz	2 GB	64 MB	2 GB/4 GB	4/2	4/3
USG5150	1 GHz	2 GB	64 MB	2 GB/4 GB	4/2	6/4

8.2 Interface Card Purchase

USG5500

The interface cards available for the USG5500 are ordered and delivered separately from the chassis.

In addition to the interface modules, electric/fiber cables may also be ordered according to the selected interface modules. For details, see Table 8-3.

Table 8-3 Available interface cards and optical transceiver modules for the USG5500

Type	Interface Card	Cable (optional)
FIC	2 x 10GE optical interface card	Single-mode or multi-mode optical fibers
FIC	8 x GE electrical interface card	Ethernet cables
FIC	2 x 10GE optical+8 x GE electrical interface card	Ethernet cables and multi-mode or single-mode optical fibers
FIC	4 x GE electrical bypass interface card	Ethernet cables
FIC	Optical bypass interface card (single-mode or multi-mode)	Single-mode or multi-mode optical fibers
FIC	8 x GE optical interface card	Single-mode or multi-mode optical fibers
DFIC	16 x GE Electrical+4 x GE optical interface card	Ethernet cables and multi-mode or single-mode optical fibers

Type	Interface Card	Cable (optional)
DFIC	18 x FE electrical+2 x GE optical interface card	Ethernet cables and multi-mode or single-mode optical fibers
DMIC	2 x 10GE optical interface card	Single-mode or multi-mode optical fibers
USB	USB-3G-E180 card	-
USB	USB-3G-EC169/EC169C card	-
USB	USB-3G-ET128/ET128-2 card	-
SFP transceiver module	Multi-mode optical transceiver module	Multi-mode optical fibers
SFP transceiver module	Single-mode optical transceiver module	Single-mode optical fibers

USG2100/2200/5100

Consider the following when purchasing the interface cards:

- If you need VLAN capability, the 5FE interface card is recommended.
- If you need to connect to the carrier through the upstream link, purchase the E1/CE1 interface card, ADSL2+ interface card, G.SHDSL interface card, FE interface card, GE interface card, SA interface card, or 3G data card.
- If you need to implement the link backup through dual upstream links, purchase the E1/CE1 interface card, ADSL2+ interface card, G.SHDSL interface card, FE interface card, GE interface card, SA interface card, or 3G data card.

NOTE
The USG2100 does not support FIC or DFIC interface card.

Table 8-4 Available expansion interface cards and optical transceiver modules for the USG2100/2200/5100

Type	Interface Card	Cable (optional)
MIC	1 x E1 interface card	• E1 75-ohm asymmetrical coaxial cables • E1 120-ohm symmetrical twisted pair cables
MIC	1 x CE1 interface card	
MIC	1 x ADSL2+ interface card	Telephone lines
MIC	1 x FE interface card	Ethernet cables
MIC	5 x FSW interface card	Ethernet cables
MIC	1 x SA interface card	• V.24 (DTE/DCE) cables • V.35 (DTE/DCE) cables • X.21 (DTE/DCE) cables
MIC	2 x SA interface card	

Type	Interface Card	Cable (optional)
		• RS449 (DTE/DCE) cables • RS530 DTE cables
MIC	1 x G.SHDSL interface card	Telephone lines
MIC	2 x G.SHDSL interface card	
MIC	4 x G.SHDSL interface card	
MIC	MIC-3G-WCDMA interface card	-
MIC	MIC-3G-CDMA2000 interface card	-
MIC	MIC-3G-TD-SCDMA interface card	-
MIC	WiFi interface card (The USG2100 do not support this card)	-
DMIC	8 x FE+2 x GE interface card	Eight 10/100M auto-sensing Ethernet electrical ports and two 10/100/1000M auto-sensing Ethernet electrical ports
FIC	2 x E1 interface card	• E1 75-ohm asymmetrical coaxial cables • E1 120-ohm symmetrical twisted pair cables
FIC	2 x CE1 interface card	
FIC	4 x E1 interface card	
FIC	4 x CE1 interface card	
FIC	8 x E1 interface card	
FIC	8 x CE1 interface card	
FIC	1 x GE interface card	Ethernet cables
FIC	4 x GE interface card	Ethernet cables
FIC	2 x FE+2 x FE combo interface card	Ethernet cables and multi-mode or single-mode optical fibers
FIC	Electrical bypass interface card (The USG2200 does not support this interface card.)	Ethernet cables
DFIC	18 x FE+2 x SFP interface card	Ethernet cables and multi-mode or single-mode optical fibers
DFIC	16 x GE+4 x SFP interface card	Ethernet cables and multi-mode or single-mode optical fibers
USB	USB-3G-E180 card	-
USB	USB-3G-EC169/EC169C card	-

Type	Interface Card	Cable (optional)
USB	USB-3G-ET128/ET128-2 card	-
SFP optical transceiver module	Multi-mode optical transceiver module	Multi-mode optical fibers
SFP optical transceiver module	Single-mode optical transceiver module	Single-mode optical fibers