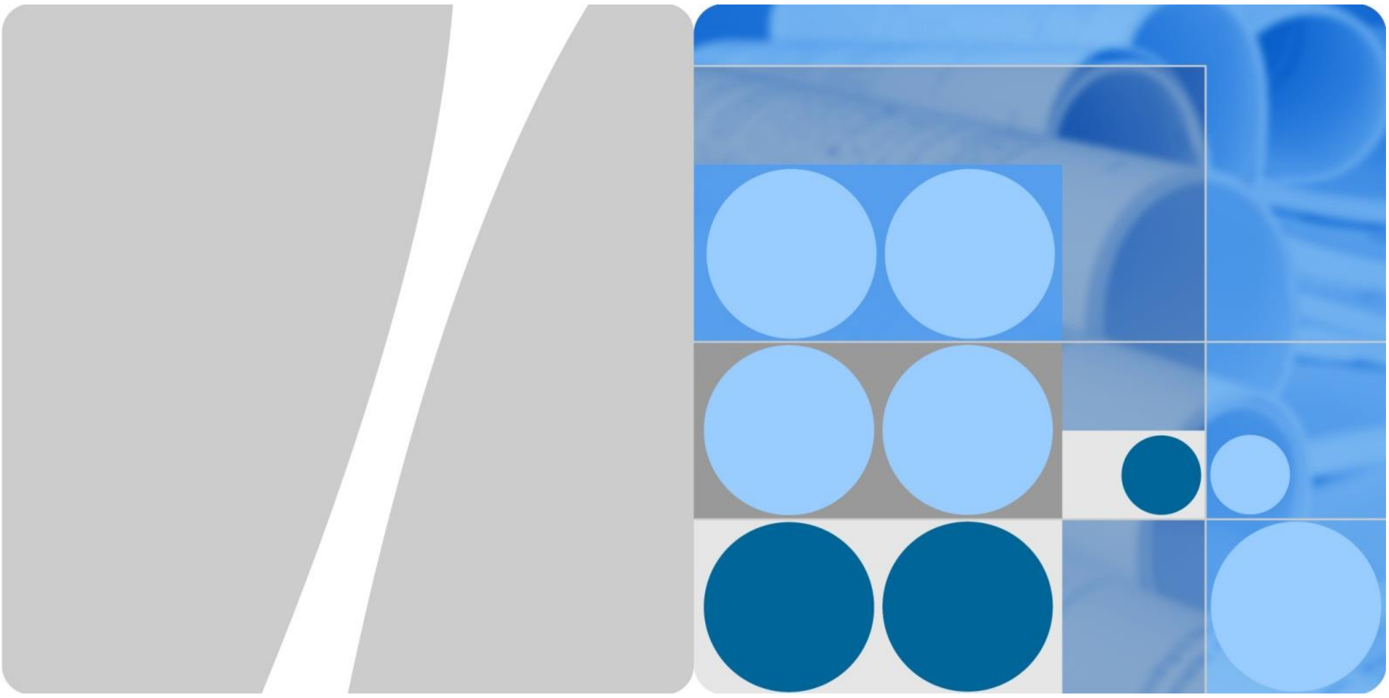


Technical Proposal Template for Huawei USG6000

Issue 01

Date 2017-03-14

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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://www.huawei.com

Email: support@huawei.com

Contents

1 Overview 1

1.1 Network Security........ 1

1.2 Threat Management........ 1

1.3 Network Security Management........ 2

1.4 New Threats on Networks........ 2

2 XX Enterprise Network Analysis 3

2.1 Status Quo of XX Enterprise Network........ 3

2.2 Service Traffic Analysis of XX Enterprise Network........ 3

2.3 Network Security Problems and Analysis for XX Enterprise........ 3

3 Network Security Requirements of XX Enterprise........ 5

3.1 Network Security Design Principles for XX Enterprise........ 5

3.2 Network Security Requirements of XX Enterprise........ 6

4 Huawei Network Security Solution 7

4.1 Network Security Solution for XX Enterprise........ 7

4.1.1 *Border Protection for Large and Medium-sized Enterprises*........ 7

4.1.2 *Intranet Control and Security Isolation* 9

4.1.3 *Border Protection for IDCs*........10

4.1.4 *VPN Remote Access and Mobile Working* 11

4.1.5 *Cloud Computing Gateway Protection Solution*........12

4.1.6 *MPLS VPN Solution* 13

4.1.7 *IPv4-to-IPv6 Transition Solutions* 14

4.2 Network Security Device Selection for XX Enterprise........14

5 Features of the Security Solutions 15

5.1 Service Traffic Analysis of XX Enterprise Network........15

5.2 Advantages of XX Enterprise's Network Security Solution 15

6 Huawei USG Series 16

6.1 USG Overview........16

6.2 Functions 16

6.2.1 Complete Security Functions Inherited from Traditional Firewalls........16

6.2.2 Advanced Content Security Defense........22

6.2.3 Flexible User Management 28

6.2.4 Fine-grained Traffic Management 29
6.2.5 IPv6 29
6.2.6 Diversified VPN Access Modes 30
6.2.7 Virtual Firewall 31
6.2.8 Interworking with the IDS 32
6.2.9 Diversified Logs and Reports 33
6.2.10 Flexible Device Management 33
6.2.11 Test and Authentication Compliance 34

7 Huawei Service 35

7.1 Service Concepts 35
7.2 Service Content 35
7.3 Service System 35

1 Overview

The popularity of the Internet has immensely boosted society development while causing lots of network security issues. Security has become a common concern among enterprises and organizations in finance, education, power supply, and transportation fields. Network security issues are about the security of networks and network security management. As the Telecom network evolves towards integration, openness, and broadband, the Telecom network becomes larger and more complex and faces various network security threats. Network security events occur frequently, such as virus, worms, malicious codes, web page tempering, and spam. Government websites are usually attacked. The single attack defense technology on the traditional firewalls cannot defend against the preceding threats.

Therefore, the Next-generation Firewall (NGFW) is developed to defend against the preceding threats. The NGFW uses the dedicated multi-core architecture platform and integrates IPS, antivirus, URL filtering, VPN, DLP, firewall functions, and Internet access behavior management. The NGFW implements the hierarchical threat defense solution.

1.1 Network Security

The Internet is vulnerable to attacks due t its openness. With attacks varying, attacking tools spreading, and Botnet/DDoS attacks emerging, the network layer is facing endless attacks. These attacks include ARP Flood attacks, ICMP Flood attacks, IP Spoofing attacks, UDP Flood attacks, Synflood attacks, Smurf attacks, Land attacks, oversize ICMP packet attacks, Fragile attacks, Ping of Death attacks, Tear Drop attacks, Ping Scan attacks, Port Scan attacks, IP source routing option attacks, and sniffing through tracert.

The network-layer attacks include bandwidth attacks, host or network device attacks, and host scanning attacks. Bandwidth attacks indicate that a great deal of attack data uses the bandwidth of normal service data, causing a feature to process the normal service data. Host or network attacks indicate that attackers attack an application interface of a host or network device, causing the host or network device to break down or fail to process normal service data. Host scanning indicates that hackers use IP sweeping or port scanning to obtain host information from network activities before intrusion.

1.2 Threat Management

Increasingly complex threats, high regulation requirements, and constant application development bring new network security problems to enterprises. Threat complexity brings more vulnerabilities to new applications and technologies and challenges to IT managers. The unified threat management platform provides a comprehensive security solution designed to work ahead of the threat.

1.3 Network Security Management

Network security management indicates that enterprises implement security zone and level division for their network sources. Network security management ensures secure network operating and improves enterprises' information security management. A security zone is a set of hosts that have the same network resource access permissions. Security zone division depends on enterprise department division. For example, security zones of different security levels are assigned for the financial department, R&D department, and marketing department. Security zone division for an enterprise simplifies network resource control and management. Then security policy management that meets enterprise management requirement is implemented to improve enterprise information security management.

1.4 New Threats on Networks

Diversified new applications bring convenience to human life as well as more security risks.

1. The identity of the user at an IP address is unclear.

   On new networks, attackers easily manipulate zombie hosts to use legitimate IP addresses to launch network attacks, or forge source IP addresses for spoofing and obtaining permissions. The source IP address of a packet does not represent the user identity. In addition, teleworking and mobile working have emerged. The IP address of a user may change at any time. Traffic control by IP address cannot meet the network requirements.

2. The port and protocol of an application are not fixed.

   Traditional network services run on fixed ports. For example, HTTP runs on port 80, and FTP runs on ports 20 and 21. On new networks, ports that are not assigned by the Internet Assigned Numbers Authority (IANA) and random ports (for example, P2P ports) are frequently used by network applications. These applications are hard to control, exhaust bandwidths, and even cause network congestion.

   Meanwhile, well-known ports are used by unfixed services. With the development of web page technologies, more and more services with different risk levels run on ports 80 and 443 using HTTP and HTTPS, for example, WebMail, web page gaming, video website, and web page chatting.

3. The packet content is uncertain.

   Single-packet detection mechanism can analyze only the security of individual packets. This mechanism cannot defend against viruses or Trojan horses during a normal access process. During the Internet access, intranet hosts may introduce worms, Trojan horses, and viruses unconsciously, which result in information leaks and losses. Therefore, network security management must identify and monitor the traffic contents, in addition to traffic control based on the source and destination IP addresses.

2 XX Enterprise Network Analysis

Through communication with XX enterprise, we have a deep understanding and analysis of its network.

2.1 Status Quo of XX Enterprise Network

This section consists of two parts. *(Note: The network throughput shall be provided):*

1. *Intranet topology of XX enterprise: You must provide the network topology without security devices if the enterprise network is newly built. This topology will be used to analyze the security solution.*
2. *Services carried by the intranet of XX enterprise, namely, internal services and egress network services.*

2.2 Service Traffic Analysis of XX Enterprise Network

[Provide service traffic analysis diagram of the live network so that customers have a more clear understanding of network security problems.]

2.3 Network Security Problems and Analysis for XX Enterprise

[This section includes the following parts (based on communication with customers and our analysis):

1. *Security risks of the XX enterprise network egress: DoS attacks and port scanning*
2. *Security zone division of XX enterprise intranet: security network resource permission management for different departments*
3. *Server protection for XX enterprise: FTP, web, mail, and database server protection for the DMZ*
4. *Security threats to XX enterprise network services: It is necessary to filter the services in various security zones and diversify enterprise management means.*

5. *Need of NAT function: As a professional NAT device, the gateway delivers excellent performance, flexible NAT functions, and diversified NAT ALGs.*
6. *Access of mobile employees: The gateway provides a great diversity of VPN access means and enables secured access to internal resources from extranets.*
7. *Intrusion risks of XX enterprise: Interworking with most IDSs in the industry implements intrusion detection.*
8. *After-event tracing of the XX enterprise network: Because the NAT function hides the internal network structure, after-event tracing will be extremely important when a social security event takes place during the access to the external network. The USG5300 provides a dedicated log server to log mappings between public and private addresses in binary format. NAT logs provide a technical means for event audit.]*

3 Network Security Requirements of XX Enterprise

[This chapter briefs and analyzes the network security problems of XX enterprise. Thorough communication with the customer and our analysis reveal that XX enterprise requires network attack defense, security zone division, and NAT...]

3.1 Network Security Design Principles for XX Enterprise

Based on the requirements of enterprise XX for network security and Huawei experience in network security, we propose that the network security design of XX enterprise must stick to the following principles:

1. Advancement: Security devices deployed in XX enterprise network must use the dedicated hardware platform and secure and professional software platform to ensure device security, which conforms to the technology development trend in aspect of advancement and maturity in the industry.
2. High availability: The network of XX enterprise is the basis for informatization of the enterprise and therefore is of vitality. Deployed at key nodes, network security devices play important roles in network stability. High availability must be considered during the network design.
3. Scalability: The fast development of XX enterprise and its changing network require that the entire network be flexible and scalable, especially for new security zones and security zone expansion.
4. Compatibility: The design standards and technical specifications of XX enterprise's security products comply with international and industry standards. XX enterprise's security products are compatible with products from many peer vendors, which helps XX enterprise maximize return on investment (ROI).
5. Minimum authorization: Security policy management of XX enterprise must comply with the minimum authorization principle. To be specific, hosts in given security zones can access only authorized resources. Resources in XX enterprise must be under control and are inaccessible to unauthorized terminals to secure the enterprise.

3.2 Network Security Requirements of XX Enterprise

Deploy a gateway to satisfy the following requirements of XX enterprise (list the requirements based on the network problems and analysis of XX enterprise):

1. *Security zone division: assign the financial department, R&D department, marketing department, and production department to different security zones.*
2. *Network attack defense: enable network attack defense at the network egress to prevent attacks from extranets and between security zones to prevent spreading of network attacks among different departments.*

...]

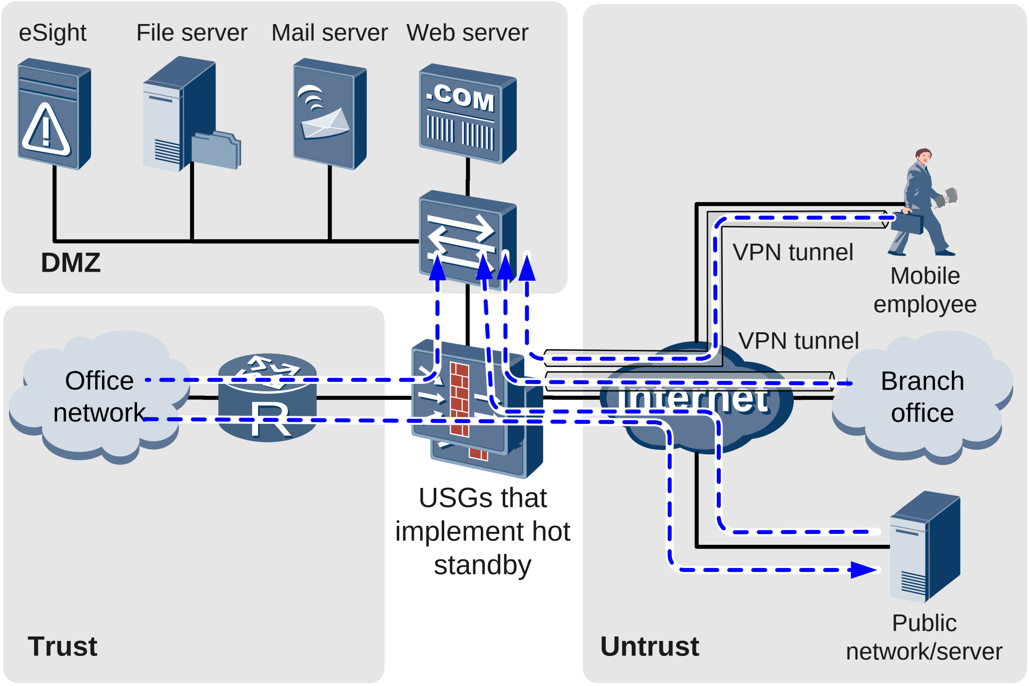
4 Huawei Network Security Solution

4.1 Network Security Solution for XX Enterprise

Choose one solution or a combination of solutions based on the analysis of XX enterprise's requirements.

4.1.1 Border Protection for Large and Medium-sized Enterprises

Figure 4-1 Typical networking of border protection for large and medium-sized enterprises



Large and medium-sized enterprises have following service features:

- Large number of employees (over 500), complex services, and various flows
- Services available to external users, such as website and mail services
- Exposure to DDoS attacks and great losses after the attacks succeed

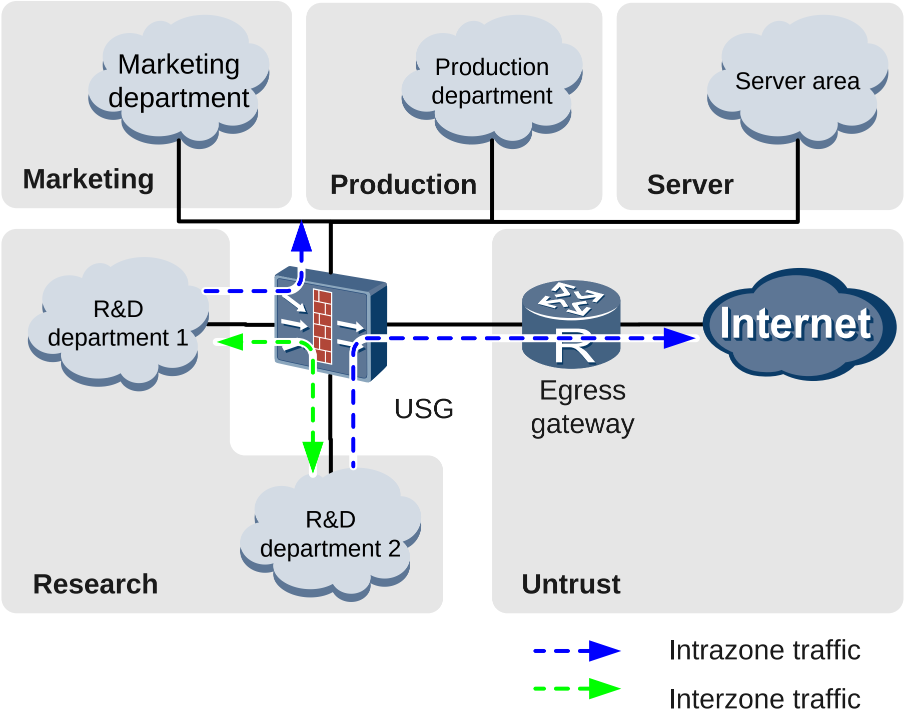
- High requirements on device reliability for service continuity when traffic is heavy or even the device is faulty

The USGs that act as egress gateways of a large and medium-sized enterprise provide the following functions:

- Assign the employee network, server network, and Internet into different security zones and configure security policies to inspect the traffic transfer between security zones.
- Implement the content security defense function based on the services to be provided to external users. For example, file blocking and data filtering are enabled on the file server in the preceding figure, mail filtering is enabled on the mail server, and antivirus and intrusion prevention are enabled on all servers.
- Implement URL filtering, file blocking, data filtering, antivirus, and application behavior control to defend against Internet threats and prevent information leaks, which ensures network security.
- Establish VPN tunnels with the devices of mobile employees and branch offices for secure communication with the headquarters across the Internet.
- Implement the anti-DDoS function to defend against heavy-traffic attacks launched by extranet hosts, which ensures the normal operating of services.
- Apply bandwidth policies to traffic between the intranet and extranet to control the bandwidth and number of connections, which avoids network congestion and defends against DDoS attacks.
- Communicate with the eLog server (to be purchased independently) that records logs about network operating. The logs help administrators adjust configurations, identify risks, and audit traffic.
- Implement hot standby to improve system availability. When a single-point fault occurs, service traffic can be smoothly switched from the active device to the standby device to ensure continuity.

4.1.2 *Intranet Control and Security Isolation*

Figure 4-2 Typical networking of intranet control and security isolation



Security levels are assigned to the subnets of the intranet of a large or medium-sized enterprise. For example, the USG isolates the R&D network, production network, and marketing network and monitors traffic among the networks to:

- Take different security measures for the service types and security risks of the networks.
- Control traffic among the networks to avoid information leaks.
- Isolate networks to prevent the spread of viruses.
- Divide networks to reduce the detection load and improve the detection efficiency for network connectivity because most traffic is generated within one network and the traffic within one network does not require much intervention.

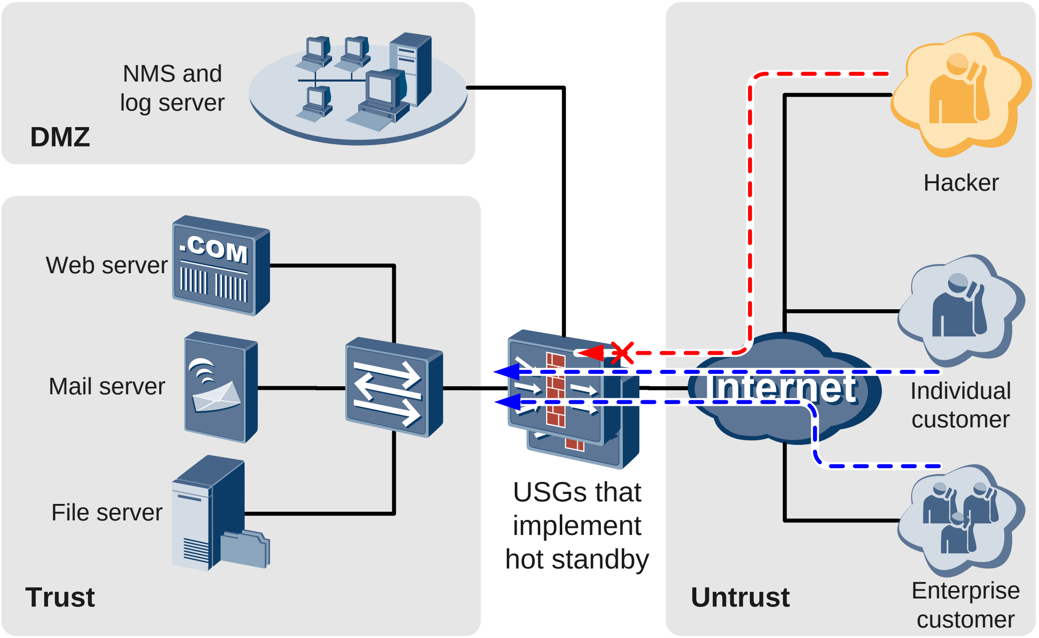
The USG that acts as an intranet border device of a large and medium-sized enterprise provides the following functions:

- Isolates networks.
- Establishes a user management system to control user access permissions.
- Assigns the networks of the same security level to the same security zone. A few security functions are deployed. For example, R&D networks 1 and 2 belong to security zone Research, and the packet filtering, blacklist and whitelist, and antivirus functions can be applied to the traffic transmitted between the two networks.
- Assigns networks of different security levels to different security zones. Security functions are deployed based on actual service requirements. For example, only some R&D hosts can access the marketing network, and the antivirus, file blocking, and data filtering functions are applied between the R&D network and the marketing, production, and server networks.

- Applies bandwidth policies to security zones to control the bandwidth and number of connections to avoid intranet congestion.
- Applies intrusion prevention, antivirus, file blocking, data filtering, URL filtering, and application behavior control functions between security zones and the Internet.

4.1.3 Border Protection for IDCs

Figure 4-3 Border protection for IDCs



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

The network structure of the IDC has the following features:

- Servers in the IDC are protected and security functions are applied based on service types.
- Servers of multiple enterprises may be deployed in an IDC and are easily taken by hackers as a target.
- The key function of the IDC is to provide network services for external users. The normal access from the Internet to servers in the IDC must be guaranteed. In this case, the border protection device must have high processing policy and comprehensive reliability mechanism and ensure the network access when attacks are launched on the IDC.
- The IDC traffic is complex. The administrator cannot adjust configurations effectively if the traffic is not unclear.

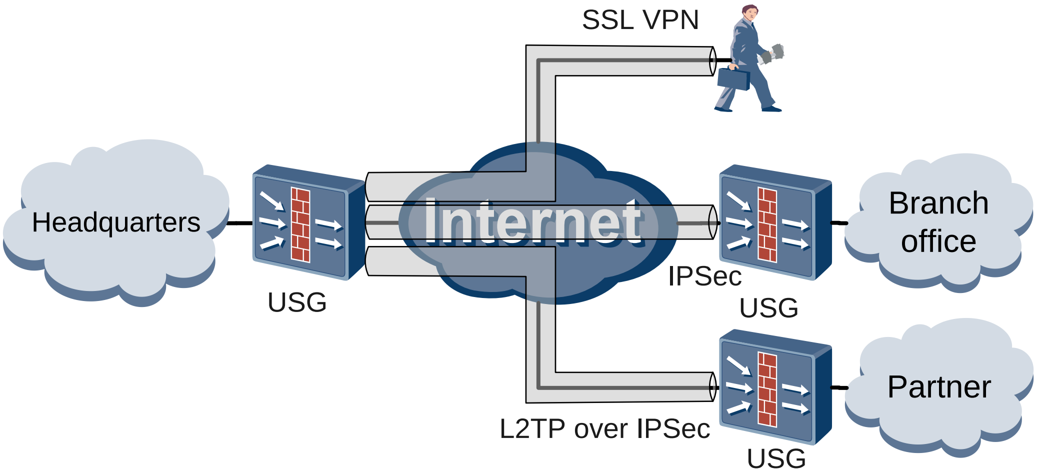
The USGs that act as border devices of the IDC provide the following functions:

- Implement the traffic statistics function to collect statistics on traffic by IP address, users, or application, which helps formulate security policies.

- Implement traffic limit by IP address or application to ensure the stable operating of servers and avoid network congestion.
- Implement the intrusion prevention and antivirus functions to protect servers from viruses, Trojan horses, and worms.
- Implement anti-DDoS and other attack defense functions to defend against attacks from the Internet.
- Implement the mail filtering function to protect mail servers on the intranet from the spam and prevent the servers from being blacklisted by anti-spam organizations due to unintentional spam forwarding.
- Implement file blocking and data filtering to prevent information leaks.
- Communicate with the eLog server (to be purchased independently) that records logs about network operating. The logs help administrators adjust configurations, identify risks, and audit traffic.
- Implement hot standby to improve system availability. When a single-point fault occurs, service traffic can be smoothly switched from the active device to the standby device to ensure continuity.

4.1.4 *VPN Remote Access and Mobile Working*

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



Nowadays, enterprises generally establish branch offices or cooperate with remote organizations around the world. Branch offices, partners, and mobile employees need to remotely access the headquarters. The secure and low-cost remote access and mobile working can be implemented using VPN technologies. Remote access and mobile working have the following features:

- Branch offices need to access the headquarters network seamlessly and implement operations uninterruptedly.
- Partners must be flexibly authorized to limit the accessible network resources and transmittable data types based on services.
- The locations, IP addresses, and access time of mobile employees are unfixed. In addition, mobile employees are not protected by information security measures. Strict access authentication must be implemented on mobile employees, and their accessible resources and permissions must be accurately controlled.

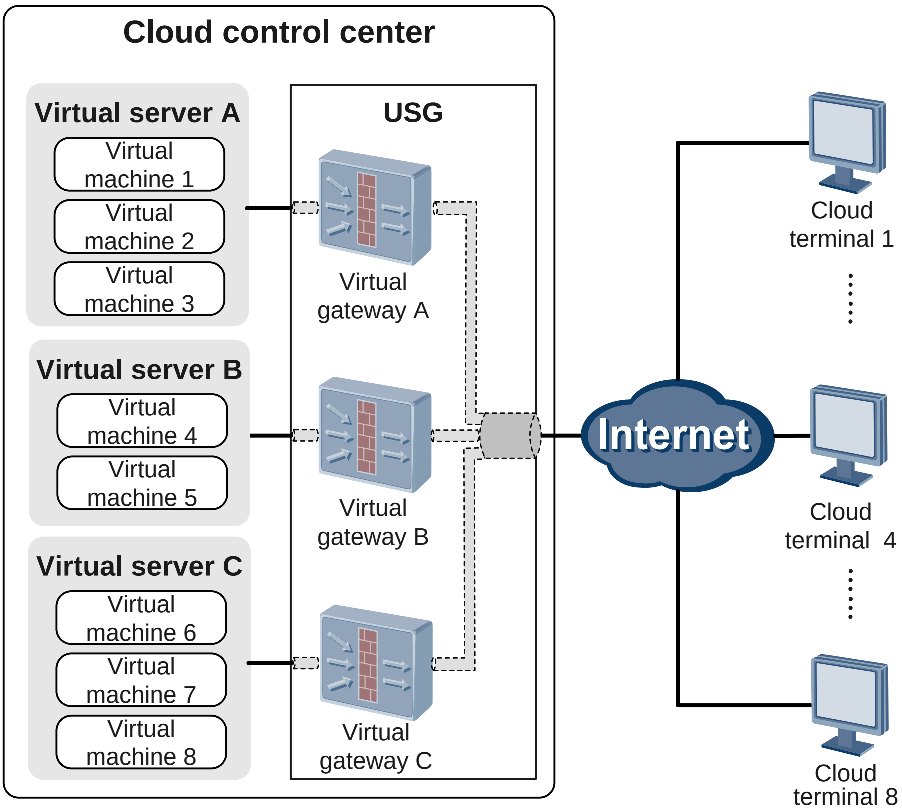
- Encryption protection must be implemented on data of remote access communications to prevent network eavesdropping, tampering, forgery, and replay as well as information leaks on the application and content planes.

The USGs that act as the access gateway of enterprise VPNs provide the following functions:

- Establish permanent IPSec or L2TP over IPSec tunnels for the branches and partners with fixed VPN gateways. If access account verification is required, L2TP over IPSec tunnels are recommended.
- The VPN client or SSL VPN technologies are used by mobile employees with variable addresses. The VPN client is for free. VPN client installation is not required. Mobile employees can use only web browsers to establish tunnels with the headquarters, which is convenient. Meanwhile, resources accessible to the mobile employees are controlled in a fine-grained manner.
- Apply the IPSec or SSL encryption algorithm to protect network data transmitted over tunnels.
- Implement access authentication on the users that access using VPN tunnels to ensure user legitimacy and access authorization based on user permissions.
- Implement the intrusion prevention, antivirus, file filtering, data filtering, and anti-DDoS functions to prevent remote access users from introducing network threats as well as information leaks.
- Implement the user behavior audit function to discover risks in time for future tracking.

4.1.5 *Cloud Computing Gateway Protection Solution*

Figure 4-5 Networking for Huawei cloud computing protection solution



Cloud computing, a new way of providing network services, requires the support of many technologies and devices. The USG can function as a cloud computing gateway on a cloud computing network.

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

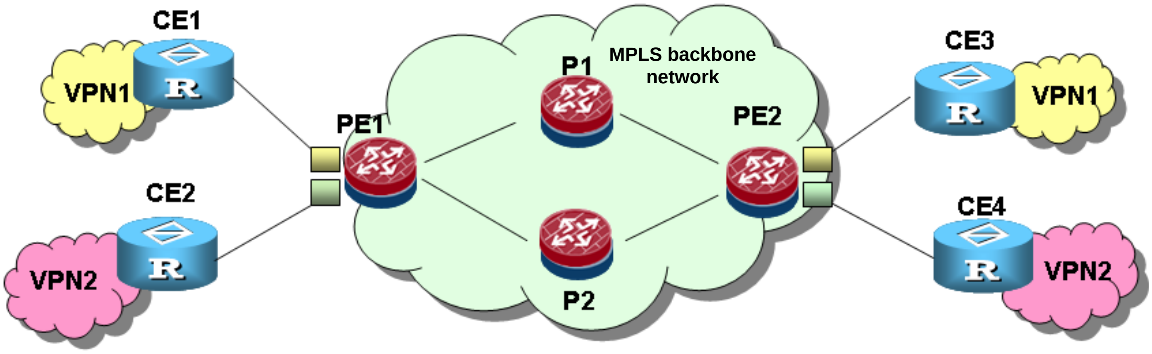
The core technology of cloud computing provides independent and complete services for a large number of users based on the server cluster, which involves multiple virtualization technologies.

The USG that acts as a cloud computing gateway of a cloud computing network provides the following functions:

- Implements the system virtualization function to divide a physical device into multiple independent logical devices. Each logical device, called a virtual system, has its own interface, system resource, and configuration file and implements traffic forwarding and security detection independently.

  Virtual systems are logically isolated and each cloud terminal has an exclusive firewall. These virtual systems share the same physical entity. Therefore, traffic forwarding between virtual systems is highly efficient.
- Offers the rapid data switching among virtual systems, protects traffic between the cloud terminal and the cloud server, and provides value-added security services for cloud computing.

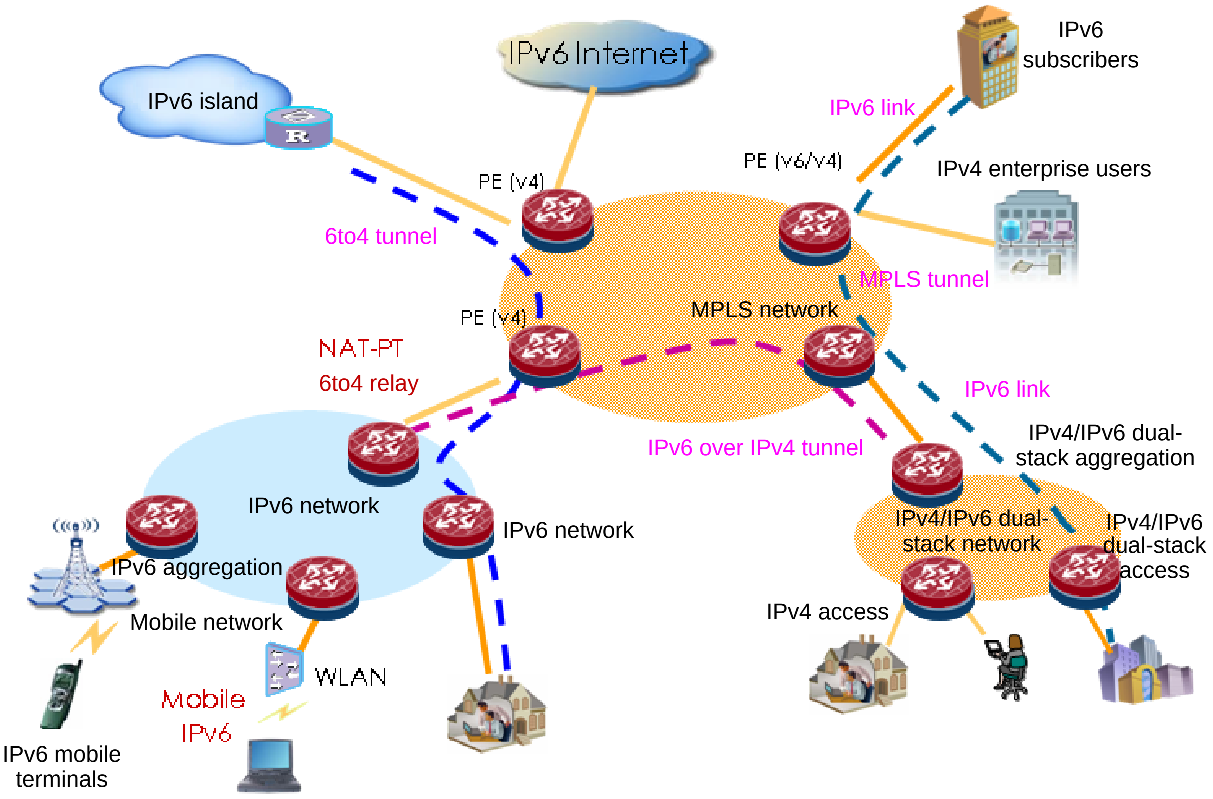
4.1.6 *MPLS VPN Solution*



The MPLS technology combines the flexible IP routing and convenient asynchronous transfer mode (ATM) label switching. MPLS adds a connection-oriented control plane into the connectionless IP network to facilitate the management and operation of IP networks. The USG supports the MPLS VPN function. It can serve as either a Provider Edge router (PE router) or a Provider router (P router). It provides the following functions:

- Multiple VRF instances
- L2TP VPN
- IPSec VPN
- Flexible VPN networking, for example, cross-domain or carrier-to-carrier.
- Standard protocol-based interconnection with the devices of other major vendors.
- CE-to-PE static routing or dynamic routing.

4.1.7 *IPv4-to-IPv6 Transition Solutions*



Because a large number of IPv4 networks already exist, IPv4 and IPv6 will co-exist for a long time along the deployment of IPv6 networks. The USG provides diversified IPv4-to-IPv6 transition solutions by providing the following technologies:

- Dual-stack technology: The USG uses IPv4 to communicate with IPv4 nodes and IPv6 with IPv6 ones. It supports three working modes: serving as an IPv6 node by running IPv6 only, IPv4 node by running IPv4 only, and a dual-stack node by running both.
- Tunneling technology: The USG enables communication between IPv6 sites across IPv4 networks and communication between IPv4 sites across IPv6 networks. It supports multiple tunneling technologies, such as IPv6 over IPv4 GRE, IPv6 manual, IPv6 over IPv4, IPv4 address-compatible automatic, and IPv6-to-IPv4 automatic tunneling.
- IPv4/IPv6 translation technology: The USG supports the translation between IPv4 and IPv6 networks. It supports Network Address Translation — Protocol Translation (NAT-PT), which performs translation between IPv4 and IPv6 packets. This technology enables the communication between IPv6 and IPv4 hosts.

4.2 Network Security Device Selection for XX Enterprise

[Deploy the USG based on the actual conditions.]

5 Features of the Security Solutions

[Analyzes the features of selected security solutions.]

5.1 Service Traffic Analysis of XX Enterprise Network

[Analyzes the service traffic of the network, which enables customers to have a clear understanding of our security solutions.]

5.2 Advantages of XX Enterprise's Network Security Solution

[Provides the advantages of the network security solution for XX enterprise based on the analysis about the service flow of the original network and the selected solution:

1. *Network topology (based on the network situations of XX enterprise)*
2. *High availability (based on the network situations of XX enterprise)*
3. *High security (based on the network situations of XX enterprise)*
4. *High* cost-effectiveness *(based on the network situations of XX enterprise)*

]

6 Huawei USG Series

6.1 USG Overview

The USG addresses the new threats posed by new networks as follows:

- Uses signatures and features instead of ports and protocols to define applications and identifies the actual attributes of packets and security risks.
- Integrates the service awareness (SA) function and employs the dedicated hardware systems to inspect the actual applications and contents of packets.
- Integrates the IPS function to ensure high performance in threat identification and blocking.
- Provides comprehensive visualized management, audit, and report functions for the network administrator to learn the actual network status and take defense measures.

The USG has the following advantages:

1. New 10-gigabit multi-core hardware platform
2. Professional content security defense
3. Integration of security, routing, and VPN functions
4. Fine-grained management by application or user
5. Visualized management and diversified logs and reports
6. Carrier-class reliability
7. Flexible scalability

6.2 Functions

6.2.1 Complete Security Functions Inherited from Traditional Firewalls

1. Security Zone Management

- Security isolation by security zone

  The security isolation function of Huawei USG is based on security zones. This design provides a good model for users to manage their networks. You can assign different interfaces of the USG to any security zone as required. Therefore, this management model is feasible for different physical topologies.

- Manageable security zones

  Many firewalls in the industry provide Trust, Untrust, and DMZ. The protection model can meet most networking requirements. It, however, cannot meet the requirements of networking that has higher requirements on security policies.

  Huawei USG provides four security zones: Trust zone, Untrust zone, DMZ, and Local zone. It has added the Local zone on the basis of the three most common security zones. The Local zone enables the security check on packets going in and out off the firewall itself, so the security protection of the firewall itself is guaranteed and enhanced. For example, by controlling the packets in the Local zone, the USG easily prevents the access from insecure zones to the firewall through Telnet and FTP.

  The USG also supports a maximum of 16 user-defined security zones. Any interface can be assigned to each one of but only one of all the security zones.

- Policy control based on security zones

  The USG allows you to design different security policy groups (ACLs) based on interzone access. Each security policy group can contain multiple independent rules. The rule system facilitates management for security policies and independent management for logical security zones.

  The policy control model based on security zones clearly defines the access from Trust to Untrust and from DMZ to Untrust zone. Therefore, this model enhances the manageability of the network isolation function.

2. NAT

- Sound address translation performance

  The USG uses connection-oriented address translation. It maintains a session entry for each connection and employs improved algorithms to achieve outstanding address translation performance. The firewall performance deteriorates little when NAT is enabled, so the USG will not become the network bottleneck when providing the NAT service.

- Flexible address translation management

  The USG provides the management function based on security zones. It divides the managed network into several logical subnets by function or security requirement. Each logical subnet is called a security zone. By default, the USG provides four security zones: Trust, Untrust, DMZ, and Local. In general, the Untrust zone connects to the Internet, the Trust zone connects to the internal LAN, and the DMZ connects to some internal servers (such as email servers and FTP servers) that provide access services. The NAT function provided by the USG is configured for the access between different security zones, which facilitates network management. For example, if the network where internal servers are deployed has sufficient IP addresses, devices can use public network IP addresses, and no address translation is required for the DMZ->Untrust interzone. The LAN, however, uses private network addresses, and address translation is required for the Trust->Untrust interzone.

  NAT can work with ACLs. An ACL defines the range of addresses that requires NAT. Therefore, it is convenient to set NAT rules on the USG, even through the rules are to be applied within the same network and even if public networks and private networks are mixed.

- Powerful intranet server support

  An intranet server, such as a web server enables extranet users to access the local intranet. Many firewalls provide a static mapping when implementing the server function. To be specific, they bind a private address to a public address, which consumes lots of valid IP addresses.

For example, the IP address of a host on a LAN is 10.110.0.0/24. The LAN is connected to the Internet using a dedicated line and has valid IP address 202.38.160.1 obtained from the ISP. If a web server with the IP address 10.110.0.1 needs to be deployed on the LAN, configure a static mapping to bind 202.38.160.1 and 10.110.0.1. If an Internet device attempts to use the address 202.38.160.1 to access the web server, the Internet device actually accesses the host at 10.110.0.1. The hosts, however, on the LAN cannot access the Internet. This is because the LAN has only one valid IP address. This IP address is used by the web server, and the other devices on the LAN cannot access the Internet. The LAN cannot provide services, such as DNS services and FTP services for devices outside the LAN.

The static binding mode has the following disadvantages:

- This mode severely wastes IP addresses. The biggest advantage of the NAT technology is that is saves IP addresses. However, IP addresses cannot be fully utilized in the static binding mode. Although this mode solves the reverse access problem in the NAT technology, it also brings the problem of address waste.
- Significant security problems may occur. Usually, a server deployed to provide services for extranets serves only a single purpose. For example, the web server only provides HTTP services for extranets. This server only needs to provide port 80. If the web server uses the static binding mode, extranet users can access any ports, including port 80, which brings security risks. For example, a server can be maintained through Telnet only from intranet devices. If the static binding mode is used, extranet users can log in to the server through Telnet.
- It is difficult to provide servers that use nonstandard ports.

  For example, if two web servers are provided, it is difficult to use the static binding mode to allow one of the web servers to use port 8080 instead of port 80.

The address translation function of the USG enables external access to internal servers at a port level. Users can configure internal servers in terms of ports and protocols for internal and external use. In the previous example, if the address translation function of the USG is used, 202.38.160.1 can be used not only as the address of the web server but also as the address of the FTP server. In addition, http://202.38.160.1:8080 can be used to provide another web server, and intranet users can use 202.38.160.1 to access the Internet.

Huawei USG provides server mappings based on ports, besides one-to-one address mapping. Moreover, each USG provides the mapping of up to 256 internal servers without affecting access efficiency.

- Powerful service support

  It is difficult to perform address translation for the packets that carries address information in its load field. The load fields of FTP packets carry address information. At present, the NAT function of the USG supports ICMP, FTP (in passive and active modes), H.323, NetMeeting, PPTP, L2TP, DNS, NetBIOS, SIP, QQ, MSN, and other special protocols. Therefore, the USG satisfies the address translation needs of the majority of network services without bringing about service bottlenecks.

  To better adhere to the development of network services, the USG provides a customized ALG function. You can customize ALGs for special applications on the CLI.

  Furthermore, during the design for the structure of the USG, special protocols that must be supported for address translation are fully considered. The structure of the USG allows the USG to support various specifically protocols and packet encryption. Owing to the great efforts for the program design, the USG now can better and quickly respond to the needs of developing special protocols, quickly respond to user requirements, and support varying services.

- PAT

  The USG supports address translation in Port Address Translation (PAT) mode. The PAT mode uses the port information of TCP/UDP, so it uses address+port during address translation to differentiate the various connections initiated by the hosts on the LAN to extranets. The PAD mode allows users on the LAN to use the same IP address to go online.

  The TCP/UDP port number range is 1 to 65,535. Ports 1 to 1024 are reserved. Therefore, in theory, the valid IP address translated in PAD mode can be used for 60,000 concurrent connections. The USG provides a no-port-limit connection algorithm, which ensures that one public network IP address can provide infinite concurrent connections. This technology breaks through the limit of 65,535 ports for Internet access in the PAT mode, better satisfies the actual needs of address translation, and saves more public network IP addresses.

- Multiple NAT ALGs

  The USG supports the following NAT ALGs:

  - NAT ALG for FTP
  - NAT ALG for the NetBIOS over TCP (NBT)
  - NAT ALG for the Internet Control Message Protocol (ICMP)
  - NAT ALG for H.323 (including T.120, RAS, Q.931, and H.245).
  - NAT ALG for the Session Initiation Protocol (SIP)
  - NAT ALG for the Real-Time Streaming Protocol (RTSP)
  - NAT ALG for the Huawei Conference Control Protocol (HWCC)
  - NAT ALG for Internet Locator Service (ILS)
  - NAT ALG for the Point-to-Point Tunneling Protocol (PPTP)
  - NAT ALG for Microsoft MSN

3. Security Policy Control

- Flexible rule setting

  The USG supports flexible rule settings based on packet characteristics so that you can:

  - Set rules based on the protocol number of a packet.
  - Set rules based on the source and destination addresses of a packet.
  - Use a wildcard to set an address range, which specifies hosts in an address segment.
  - Specify a source/destination port for UDP or TCP.
  - Set a port range for the source and destination ports using the methods such as greater than, equal to, between, or not equal to.
  - Specify a type and code of ICMP packets and set a rule for each type of ICMP packets
  - Set flexible rules based on the TOS field of IP packets.
  - Use the addresses of multiple packets to form an address group. Rules can be set based on address books.

- High-speed policy matching

  A security policy of a firewall consists of many rules. Therefore, policy matching affects the forwarding efficiency of firewalls.

The USG uses a dedicated algorithm to accelerate ACL rule matching. The algorithm ensures that the USG can efficiently forward packets even when applied security policies have many rules. When the system searches for a matching rule among thousands of ACL rules, the system performance is almost not influenced and the processing speed maintains the same, which ensures high-speed ACL rule query and improves the overall system performance.

- Binding of MAC addresses and IP addresses

  The USG creates bindings of Media Access Control (MAC) addresses and IP addresses based on users' configurations. A packet whose IP and MAC addresses do not match is discarded. A packet destined for an IP address is forcibly sent to the associated MAC address when passing the firewall. This mechanism can effectively defend against IP spoofing attacks.

- Dynamic policy management — blacklist

  The USG can blacklist the source IP addresses of suspected packets. Then the USG can discard the packets that match entries in the blacklist, which prevents the attacks from malicious hosts.

  The USG supports the following modes of maintaining a blacklist:

  - Manually add entries to the blacklist to implement proactive defense.
  - Automatically add blacklist entries through attack defense to implement intelligent protection.
  - Set a whitelist, which allows blacklisted hosts to access specific network resources. For example, users are allowed to access the Internet from a host even if the host is blacklisted.

  The blacklist technology a dynamic policy technology. The USG discovers attacks and updates the blacklist dynamically. Therefore, abnormal traffic is discarded once detected.

4. Attack defense

- Necessary conditions for anti-DoS

  DoS attacks are common attacks over the Internet. During a DoS attack, an attacker sends various attack packets to devices to cause network breakdown or congestion. IP communication is connectionless. Taking advantage of this feature, attackers invent various attack means. Launching DoS attacks is extremely simple. For example, a PC and a packet sending tool are enough. Consequently, DoS attacks prevail the Internet and greatly compromises intranets and even backbone networks, causing serious network accidents. Therefore, an excellent anti-DoS capability is indispensable to firewalls.

  A sound anti-DoS attack system should have the following features:

  - Has rich attack defense means to defend against DoS attacks.
  - Has high processing performance. A DoS attack causes traffic bursts. Therefore, firewalls must have high traffic processing performance to defend against DoS attacks. Otherwise, the firewalls are broken down by the attacks. Network breakdown is an important aim of DoS attacks. Therefore, firewalls must have high traffic forwarding and processing capabilities. The number of new connections per second becomes an important index for network performance. During DoS attacks, attackers randomly change source addresses contained in sent packets. Therefore, all connections between the attackers and target devices are newly built.
  - Has an accurate attack identification capability. When processing DoS attacks, many firewalls can only ensure that the traffic volume is within the acceptable range but cannot accurately identify attack packets. In this way, the firewalls are not broken down but packets sent by authorized users to go online may be denied. As a result, the firewalls cannot effectively defend against DoS attacks.

The USG has taken all the preceding aspects into consideration, so it has prominent advantages over counterpart products in anti-DoS performance and features.

- Rich anti-DoS means

  Based on the features of data packets and the specific means of DoS attacks, the USG can defend against DoS attacks, such as ICMP flood, SYN flood, and UDP flood attacks.

  The USG identifies a dozen of common attack types, many among which may result in DoS attacks. The USG proactively detects and isolates these attacks and therefore prevents the intranet from being attacked. With these anti-DoS means, the USG constructs a secure defense system against DoS attacks.

  The USG uses differentiated defense technologies for different attacks. Therefore, it provides dedicated DoS attack defense and delivers a comprehensive defense feature.

  In addition to the consideration of attack means, the USG has enhanced its usability and network adaptability. Users can set a defense scope to a specific host or all hosts in a security zone.

- Advanced defense system through TCP proxy

  The USG uses TCP proxy to prevent DoS attacks, such as SYN flood attacks, which may quickly use up all resources of a server and cause the server to crash. Common anti-DoS technologies cannot identify valid packets and attack packets when attacks occur. The USG uses transparent TCP proxy to defend against DoS attacks. It permits normal packets and directly discards attack packets.

  Some attackers establish complete TCP connections to use up server resources. The USG can implement the enhanced proxy function. After establishing a connection with a client, the USG checks whether the client has any follow-up data to transmit. The USG establishes a connection with the server only when the client has data to transmit. The enhanced proxy function ensures that the USG can discover the DoS attack launched by an attacker that uses the three-way handshake to establish a TCP connection.

- Scanning attacks

  Scanning and sniffing attacks identify active systems on a network by ping scanning, including ICMP and TCP scanning, to accurately locate targets. Then attackers can detect the monitored potential services and operating systems by scanning TCP and UDP ports. Through scanning and sniffing, attackers can learn about potential security vulnerabilities of and service types provided by the target system, preparing for further attacks.

  The USG can detect scanning and sniffing packets through comparative analysis to prevent subsequent attacks. Scanning and sniffing attacks include address scanning, port scanning, IP source routing options, IP route record options, and network structure sniffing through tracert.

- Malformed packet attack defense

  The USG can identify and defend against various malformed packet attacks, including Land, Smurf, Fraggle, WinNuke, ICMP redirect or unreachable packet, invalid TCP flag bits (such as, ACK, SYN, and FIN), Ping of Death, and Tear Drop attacks.

5. ASPF

The USG provides the ASPF technology. ASPF is an advanced packet filtering technology used to check packets and monitor the status of connection-oriented application layer protocols. The USG uses packet content-based access control to detect some attacks targeting the application layer, including FTP command fields, SMTP commands, and Java applet and ActiveX controls on HTTP.

ASPF provides deep detection based on session management. ASPF uses session management information to maintain access rules. ASPF stores session status information in the session management module. The session status information cannot be stored using static access lists. Session status information can be used to intelligently permit or deny packets. When a session terminates, the session management module deletes this session from its session table, and the USG also closes the session.

ASPF can intelligently detect the three-way handshake for connection establishment and the handshake for connection removal. Detection on handshakes and connection removal ensures that normal TCP-based access can normally proceed and the packets of incomplete TCP handshake connections are directly denied.

The ACL-based IP packet filtering technology is widely used for access control. This technology is simple but lacks flexibility. This technology cannot well protect complex networks. For example, for multi-channel protocols, such as FTP, it is rather difficult to configure the rules of the firewall. FTP has a TCP control channel with predefined ports and a dynamically negotiated TCP data channel. Users cannot obtain the port number of the data channel when configuring security policies for a common firewall. As a result, users cannot determine the ingress of the data channel, and no accurate security policies can be configured. ASPF can resolve this problem. It detects application-layer packets and dynamically creates or deletes rules based on packet contents.

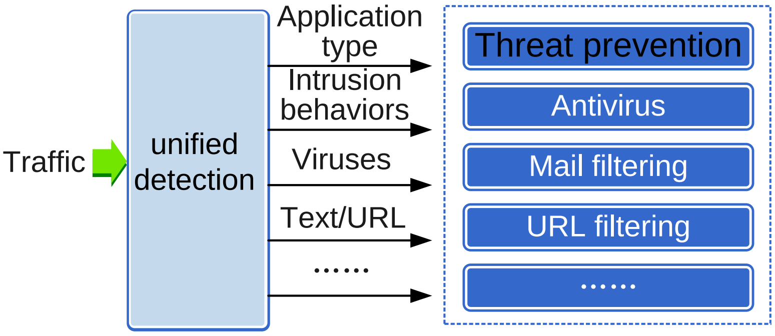
ASPF enables the USG to support multiple connections over one control channel and allows users to define various security policies in complex networking. Many application protocols, such as Telnet and SMTP use standard or well-known ports for communications, but most multimedia application protocols (such as H.323 and SIP) and other protocols (such as FTP and NetMeeting) use designated ports to initialize a control connection and then dynamically select ports to transmit data. Port selection is unpredictable. An application may use more than one port at the same time. ASPF monitors ports used by each connection of each application. Opening a proper channel allows session data to get in or out of the firewall. The channel is closed upon session termination, so that effective access control can be exercised for the applications that use dynamic ports.

When a packet passes through the USG, ASPF matches the packet with specific access rules. If permitted by the rules, the packet is permitted. Otherwise, the packet is silently discarded. If this packet is used to establish a control or data connection, ASPF dynamically modify rules. The return packet is permitted as long as the packet matches one valid rule. The status table is updated when the return packet is processed. If a connection is closed or expires, the status entry to which the connection corresponds is deleted, which prevents unauthorized packets.

6.2.2 Advanced Content Security Defense

1. Unified Detection Mechanism

The unified detection mechanism of the USG provides effective content security function and high performance even when these functions are completely enabled. The unified detection mechanism is used to obtain all data for content security functions by inspecting packets once, which greatly enhances device performance.



2. Antivirus

The antivirus function scans the files transmitted over networks and records or removes the identified viruses in the files. A virus is a set of self-replicable instructions or program codes compiled independently or embedded in computer programs to adversely affect the computer use by damaging specific functions or data of the computer. Commonly, viruses are embedded in files and are spread through emails, web pages, and file transfer protocols. If a host on an intranet is infected with viruses, the entire system may crash, relevant services may be interrupted, and important data may be leaked, bringing tremendous loss to enterprises. The antivirus function of the USG detects and scans file transfer and file sharing protocols that are commonly used to transfer viruses. The USG blocks multiple detection-evasive mechanisms used by viruses, enhancing the antivirus capability of the network. The antivirus capabilities of the USG are as follows:

- Support of abundant protocols and applications at the application layer

  The USG supports virus scanning for files transmitted using HTTP, FTP, SMTP, POP3, IMAP, NFS, and SMB. In addition, the USG supports exception actions set for specific HTTP-based applications.

- Virus scanning for compressed files

  The USG supports ZIP or GZIP file decompression before it performing virus scanning.

- Signature database with massive signatures

  The predefined virus signature database of the USG is used to detect over 3000 mainstream virus families, covering over one million common viruses. The virus signature database with massive signatures ensures the advanced virus detection capability of the USG. The professional virus analysis team of Huawei traces and analyzes the latest type of viruses and updates the virus signature database for network administrators. Therefore, the USG obtains the latest signature database and has the capability to identify the maximum number of viruses.

- Different defense measures for traffic flows of various kinds and antivirus policies based on application and virus exceptions

  With security policies, administrators can create and apply fine-grained defense policies for different traffic flows to provide differentiated network protection. In addition, the administrator can adjust the antivirus policy to ensure normal service packet transmission by configuring additional protection actions for HTTP-based applications or adding false-positive viruses to the virus exception list.

3. Intrusion Prevention

The intrusion prevention function prevents attacks or intrusions, such as cache overflow attacks, Trojan horses, backdoor attacks, and worms, at the application layer. The intrusion prevention function enables the USG to monitor or analyze system events, detect attacks and intrusions at the application layer and takes actions to stop intrusion in real time. The intrusion prevention capabilities of the USG are as follows:

- Different deployment modes and unique defensive measures for each type of traffic flows

  The USG can be deployed in either in-line and off-line mode. When deployed in in-line mode, the USG can act as an IPS device. It detects threats in real time and blocks the transmission of specific traffic flows to protect the intranet. When deployed in off-line mode, the USG can act as an IDS device in off-line mode. It records suspicious events and informs the administrator of these events but does not block the suspicious traffic. With security policies, administrators can create and apply fine-grained defense policies for different traffic flows to provide differentiated network protection.

- In-depth application-layer packet resolution

  The USG has a constantly updated application signature database. It performs in-depth packet resolution on the traffic flows from thousands of common applications for attacks and intrusions. Based on application-specific security policies, the USG takes corresponding actions to the traffic flows from different applications. In this case, the administrator can flexibly deploy the intrusion prevention function.

- Threat detection after packet fragment reassembly and TCP stream reassembly

  Some attacks make use of IP packet fragments and TCP stream reassembly to evade threat detection. To tackle this problem, the USG reassembles the IP packet fragments into original packets or streams into original traffic flows before performing threat detection.

- Signature database containing thousands of signatures, including the user-defined ones

  The IPS device uses signatures to detect attack traffic. Therefore the capacity of the signature database represents the threat identification capabilities. To cope with endlessly emerging attacks and threats, Huawei has established a professional security team to closely trace the security bulletins of renowned security organizations and software vendors, analyze and verify threats, and generate the signature database for protecting software systems, including operating systems, application programs, and databases. In addition, the USG captures the latest attacks, worms, viruses, and Trojan horses, extracts signatures from them, and determines the trend of the threats with the help of the globally scattered honeynet. A honeynet is a website that lures hackers and collects data for producing signatures. Based on the preceding features, Huawei can release the signature of a virus that attacks a newly identified vulnerability and update the signature database and inspection engine in the shortest time. The signature can prevent all attacks, known or unknown, that take advantage of the vulnerability, delivering zero-day protection. The predefined signature database helps the USG identify thousands of attacks at the application layer, whereas the constant updates of the signature database ensure that the USG identifies and defends against latest attacks and threats. In addition, the administrator can define signatures of their own as required to enhance the intrusion prevention function of the USG.

- Low false positive rate

  False positive rate is an important metric of the accuracy of signatures and the quality of the signature database. False positives compromise legitimate services and bury valuable information in the false information, making it harder to isolate real attacks. False positives are usually caused by inaccurate signatures or detecting mechanisms. Huawei has a host of security professionals and data sources to analyze samples, create signatures, and perform false negative tests to achieve near-zero false positive rate. Due to the extremely low false positive rate, a large percentage of the signatures are enabled by default on the USG to maximize protection without compromising legitimate services. The administrators do not need to check a bunch of logs for false negatives or to determine whether some signatures should be disabled.

4. Data loss prevention

Data loss prevention (DLP) prevents the leak of specified data or information assets. Leaks are a violation of the security regulations and policies imposed by enterprises on their networks. The main purpose of DLP is to protect the key data of enterprises and individuals. DLP is implemented through a set of technologies to defend against data leaks of various kinds. The DLP function of the USG prevents data leaks. For example, data leaks may occur when

- Secret data is transmitted from an intranet to an extranet through network communication tools.
- Most data leaks are intentionally or accidentally caused by employees of enterprises.
- Hackers from extranets invade the hosts on the intranet, obtain the permissions to control them, and even monitor their running status for a significant time.
- The hosts on the intranet are infected with viruses, Trojan horses, or other spyware and the secret data stored on the hosts is automatically searched and spread by these malicious programs.
- The hackers listen to or intercept the communication between the hosts on the intranet and those on the extranet.

To prevent data leaks, the USG addresses the possible data leak causes as follows:

DLP		
Data Leak Channel	**Technology**	**Description**
Through file transfer protocols, such as HTTP, FTP or network communication tools, such as the IM software	Application identification, file blocking, and data filtering	The USG uses application identification to perform in-depth packet inspection on network communication applications and file transfer protocols and identify the files and information included inside the packets. Data filtering helps filter out files based on the keywords they contain, whereas file blocking helps filter out files based on the file properties such as file type.
Through texts or email attachments	Mail filtering, file blocking, and data filtering	Mail filtering helps filter out email messages based on the addresses of email senders and receivers and the size and number of email attachments. File blocking helps filter out email messages based on the types of attached files. Data filtering helps filter out email messages based on the keywords in email addresses, subjects, bodies, and the names of the attached files.
Through hacker invasion	Intrusion prevention	The USG monitors the network application layer attacks and intrusions, blocks the intrusions from extranets, and prevents data leaks from within.

DLP		
Data Leak Channel	**Technology**	**Description**
Through the hosts infected with viruses	Antivirus	The USG scans and identifies Trojan horses and other spyware to prevent the infection and spread of viruses with the similar intentions.
Through eavesdropping during the normal data transmission between the intranet and extranet	VPN	The USG implements the VPN encryption technology to prevent network eavesdropping, tampering, forgery, and replay.

In addition to proactive defense measures, the USG monitors, manages, traces, and collects evidence of data leaks through application behavior audits. The preceding technologies of the USG plus the management of storage devices, file encryption, user authentication, and user authorization ensure the E2E data protection and form a complete DLP solution.

5. Web Security Defense

The development of cloud technology precipitates the migration of more and more applications from desktop to the Web. The migration also turns the web from a pure web browsing service to a comprehensive platform that integrates multiple services related to finance, social networking, music, video, and online games. The enrichment and development of the web service bring various security threats. To avoid possible harms, the combination of multiple technologies can protect websites and control the access to them.

Illegal and malicious websites are the most significant problems related to the web. An illegal website is one that contains information, such as violence or pornography and has been considered illegal by local laws and regulations or the management system of enterprises. Websites of this kind adversely affect social stability, lowers the work efficiency, and consumes the bandwidth of and resources on the intranet. A malicious website is the one that hosts Trojan horses and phishing web pages, implants Trojan horses into the access hosts, initiates SQL injections and cross-site scripting attacks, takes advantage of the vulnerabilities in the browsers or operating systems, and scam money from victims. Websites of this kind may cause significant loss to users or enterprises. A prominent feature of malicious websites is their capability to cause significant loss to users without their awareness.

URL filtering helps control the access to URLs. The administrator can define their own URL categories and corresponding actions based on the URLs in the predefined URL category database of the USG. In addition, the URL categories provided by the USG contain a large number of known URLs of the Trojan horses and phishing websites. With the preceding data, the USG automatically searches for the URLs accessed by users in the URL category database and takes appropriate actions.

To cope with the dynamically changed URLs and the constant increase of these URLs, the USG traces the changes on the Internet and updates the URL category database in real time to constantly enhance the URL filtering function. Besides, the administrator can establish a local URL category searching server and use the server to learn complete URL categories from the searching server of Huawei. Then, local USGs perform URL queries on the local searching server. This deployment scheme reduces bandwidth consumption, improves the query speed, and ensures the availability of the query service even when the USG is disconnected from the Internet.

6. Application Behavior Control

Application behavior control over specific network behaviors on enterprise networks helps avoid security risks and improve management efficiency. The network serves as an indispensable platform and instrument for modern enterprises. Network abuse causes many problems:

- Browsing and downloading non-work-related web content during working hours lowers down work efficiency and wastes network resources of enterprises.
- Outgoing transfer of texts and files by employees may leak secret information from enterprises.
- Posting inappropriate opinions violated local laws and regulations or the management policies imposed by enterprises causes significant loss to corporate image or interests.

Application behavior control of the USG effectively monitors and controls network access behaviors, reduces the loss caused to corporate interests, and improves work efficiency of enterprises. The details on the control are as follows:

- HTTP behavior control
  - Supports the blocking the operations, such as message post, form submission, and user login, through HTTP POST.
  - Supports the blocking of requests to browse web pages.
  - Supports the blocking of network access through HTTP proxy.
  - Supports the alerting and blocking of file upload and download through HTTP based on the sizes of the uploaded and downloaded files.
- FTP behavior control
  - Supports the alerting and blocking of file upload and download through FTP based on the sizes of the uploaded and downloaded files.
  - Supports the blocking of the operation of deleting files from an FTP server.

7. Anti-spam

The anti-spam function blocks junk mails based on the IP address of the outgoing mail server and email content. Any unsolicited email message sent to user inbox can be regarded as the junk mail. However, massive junk mails nowadays bring adverse impacts to the network as follows:

- Congest the mail server and lowers the performance of the entire network.
- Infringe upon the privacy, consume the storage space of the inbox, and waste the time, efforts, and money of receivers. Specific junk mails use the email addresses of others as the senders' email addresses, destroying the reputation of the actual owners of these email addresses.
- Contain Trojan horses and viruses and turn to be network attacks if they are manipulated by hackers.
- Severely affect the credibility of an ISP. The hosts that frequently send junk mails are listed in the international junk mail database by its supervisor ISP. In this case, the hosts cannot access certain resources on the network. If the current ISP does not build a comprehensive anti-spam mechanism, the users who receive junk mails may turn to other ISPs.
- Spread false and pornographic contents, causing damages to the society.

The USG supports the following mail filtering mechanisms:

- Controls the permitted mail server through locally defined blacklists and whitelists.

- Checks whether a mail server is the one that usually forwards junk mails through a remote RBL query server on the Internet. The RBL query server provides a comprehensive and constantly updated list of mail servers that forward junk mails.
- Filters emails based on the sender, subject, and the keywords in the mail body.

6.2.3 Flexible User Management

IP addresses no longer reflect user identities, which poses a security risk. However, user-specific management delivers an effective solution to this issue. In the initial phase of network development, an IP address was a unique identifier of a specific host on the network, and the firewall performs traffic control based on IP addresses. However, the popularization of mobile working and teleworking makes the integrated management of IP addresses a demanding task. Furthermore, IP addresses are included in the packets in plain text and can be easily tampered with. Therefore, an increasing number of network frauds are implemented through IP spoofing. The USG uses user-based security measures to resolve the preceding problems. A user needs to enter the user name and password to access the network from a host. The user is allowed to access the network only after passing the authentication. The user name and password represent the identity of the user. The administrator can configure policies based on users on the USG, which helps implement fine-grained security policy deployment, such as resource-based authorization, security protection, and traffic management policies.

The USG provides the following functions:

- Storage and management for user information, such as user names and passwords
  - You can create users and user groups on the USG. The USG supports tree-shaped organization management and group nesting and can meet the organization requirements of most enterprises.
  - You can manage users and user groups on a third-party authentication server and synchronize or import the data from the server to the USG. The authentication servers include AD, RADIUS, LDAP, HWTACACS, SecurID, and TSM servers.
- User authentication
  - Local authentication Users are created and managed on an authentication server. The USG pushes the authentication page to users' browser. The authentication server locally authenticates the users.
  - Authentication through proxy. Users are created and maintained on a third-party authentication server. The USG functioning as a proxy forward users' authentication requests to the server and obtain the authentication results. User names and organization structures need to be imported to the USG from the server to allow the USG to apply policies to users.
  - Synchronization with the AD server The USG can obtain the authentication results from the AD server after the AD server authenticates users. No further authentication is required.
  - Whether second authentication is performed for users that access the intranet through VPN tunnels is determined by access mode.
- Permission control and traffic management

  You can create or import the following policies:
  - Security policy: controls network access permissions and provides content security.
  - Bandwidth policy: controls the used bandwidth and number of connections and adjusts the traffic forwarding priorities of specific users.
  - Policy-based routing: specifies the outgoing interface of user traffic.
  - Audit policy: audits users' online behaviors.

6.2.4 Fine-grained Traffic Management

Network services are ever-increasing, but network bandwidth is not. Therefore, bandwidth usage must be controlled to reduce the bandwidth for low-priority services and ensure available bandwidth for high-priority services.

Currently, common problems that administrators encounter are as follows:

- P2P applications consume most bandwidth.
- DDoS attacks make services unavailable to legitimate users.
- Stable bandwidth usage or number of connections cannot be ensured for certain special services.
- Overload traffic degrades device performance and user experience.

To resolve the preceding problems, the USG provides the traffic management technology to:

- Reduce the bandwidth for P2P traffic by allocating the bandwidth and number of connections based on IP addresses, users, applications, or time.
- Limit the bandwidth for security zones or interfaces to prevent overwhelming traffic from degrading or paralyzing servers and network devices.
- Set guaranteed and maximum bandwidths for applications to ensure proper bandwidth allocation and the availability of special services. The powerful application identification capability enables the USG to implement fine-grained bandwidth management.

The USG flexibly allocates bandwidth using bandwidth policies. Each bandwidth channel represents a bandwidth range or connection number range. Each bandwidth policy assigns a bandwidth channel for the traffic of a specific type.

- If multiple bandwidth policies share a bandwidth channel, traffic flows defined in the policies obtain the bandwidth and number of connections through preemption to ensure the full use of the network resources. In addition, the maximum bandwidth for each IP address or user can be restricted to ensure smooth global traffic transmission and the network access experience of individual users.
- If a bandwidth policy takes over a bandwidth channel, the traffic flow of certain special services or hosts defined in the policy is not affected by other traffic flows. The takeover of a bandwidth channel ensures the availability of high-priority services.

6.2.5 IPv6

The USG supports Internet Protocol Version 6 (IPv6) and various IPv6 networking modes and effectively secures IPv6 networks. IPv6 is a second-generation standard protocol of network-layer protocols. It is designed by the Internet Engineering Task Force (IETF) as an upgraded version of IPv4. Different from IPv4 with its IP address as 32 bits, the IP address of IPv6 becomes 128 bits. IPv6 solves the lack of IP addresses. Additionally, after IPv6 is widely applied, the number of routing entries in the routing table of routers on the network decrease, improving the packet forwarding rate. The following types of IPv6 technologies are involved in IPv6 network construction:

- Basic IPv6 technologies used for IPv6 host communication
- IPv6 transition technologies used for communication between IPv6 hosts and IPv4 hosts during the transition from IPv4 networks to IPv6 networks

1. Basic IPv6 technologies

- IPv6 address

  - Supports both IPv4 and IPv6 protocols.
  - Parses IPv6 packet headers and forwards packets based on the IPv6 addresses in the headers.
  - Supports automatic and manual IPv6 address configuration and IPv6 neighbor discovery.
  - Supports ICMPv6, DNSv6, DHCPv6, and PPPoEv6.
- IPv6 routing
  - Supports IPv6 static routes, policy-based routes, and routing policies.
  - Supports RIPng.
  - Supports OSPFv3.
  - Supports BGP4+.
  - Supports IPv6 IS-IS.

2. IPv6 transition technologies

The following transitional technologies are used for the evolution from IPv4 to IPv6:

- IPv6 over IPv4 tunneling: allows two IPv6 networks isolated by IPv4 networks to communicate. In the early phase of IPv6 development, few IPv6 networks exist and are usually indirectly connected. The IPv6 networks need to communicate based on existing IPv4 networks. IPv6 over IPv4 tunnels are established between the edge devices of IPv4 networks and IPv6 networks, which allows IPv6 packet transmission over the IPv4 networks.
- IPv4 over IPv6 tunneling: allows two IPv4 networks isolated by IPv6 networks to communicate. In the late phase of IPv6 development, most networks are IPv6 networks. Only a few IPv4 networks exist and are isolated by IPv6 networks. IPv4 over IPv6 tunnels are established between the edge devices of IPv6 networks and IPv4 networks, which allows IPv4 packet transmission over the IPv6 networks.
- NAT64: When IPv6 networks and IPv4 networks coexist, IPv6 hosts and IPv4 hosts need to communicate. NAT64 can perform translation between IPv4 addresses and IPv6 addresses. For example, NAT64 translates the source and destination addresses of a packet sent by an IPv6 host to an IPv4 host to specific IPv4 addresses so that the packet can be transmitted over IPv4 networks. Then NAT translates the source and destination addresses of the response packet sent by the IPv4 host to specific IPv6 addresses so that the IPv6 host can receive the packet. NAT64 enables IPv4 hosts and IPv6 hosts to communicate.

The USG provides IPv6 network security functions, besides overall IPv6 networking technologies. The USG supports security policies based on IPv6 addresses to protect IPv6 networks. The USG implements packet filtering and content security inspection on packets based on the IPv6 addresses.

6.2.6 Diversified VPN Access Modes

- **IP VPN services**

  With the IP Security (IPSec) mechanism, Huawei USG provides services, such as access control, connectionless integrity, data source authentication, anti-replay, and encryption, and data flow classification and encryption for communications parties. The USG uses Authentication Header (AH) and Encapsulating Security Payload (ESP) to protect data packets transmitted over the IP or upper layers and supports the tunnel encapsulation mode.

In addition to providing IPSec VPN to set up highly reliable and secure transport channels, the USG provides Layer 2 Tunneling Protocol (L2TP) and Generic Routing Encapsulation (GRE) for various VPN applications:

- IPSEC VPN
- L2TP VPN
- GRE VPN
- L2TP over IPSec VPN
- GRE over IPSec VPN

An intranet VPN is established using firewalls for communication between the headquarters and branch offices over the public network. An access VPN is established for Small Office/Home (OfficeSOHO) or users to access the headquarters over the Public Switched Telephone Network (PSTN)/Integrated Services Digital Network (ISDN). An extranet VPN is established for secure communication between an enterprise and its partners/customers.

The USG supports the following VPN functions to meet various networking requirements:

- VPN connections between the headquarters and branch offices, which ensures the confidentiality of the data transmitted between the headquarters and branch offices.
- VPN connections between remote users and an intranet

  Remote users can dynamically access the intranet using L2TP over IPSec or SSL VPN.
- VPN connection between mobile phones and an intranet

  Users can access an intranet over the VPN tunnels established based on VPN clients or USGs between their iPhone/iPad/Android devices and the intranet.
- CA certificates for IPSec VPN, SCEP, and OSCP, which allows dynamic certificate download and display.
- Dual homing to a VPN

  The USG dynamically triggers VPN tunnel establishment. When dual-homed to a VPN, the USG can trigger VPN tunnel establishment and deletion.
- Hot standby for VPN services

  Two USGs can implement not only hot standby but also IPSec VPN backup. If one USG becomes Down, the other USG takes over services without reestablish VPN tunnels, which implements uninterrupted user data transmission.

6.2.7 Virtual Firewall

The virtual firewall function logically divides a physical firewall into multiple independent virtual firewalls. Each virtual firewall has its own administrator, routing table, and security policies.

The virtual firewall function applies to the following scenarios:

- Device Leasing: Virtual firewalls can be leased to small enterprises so that they can protect their networks without paying for physical security devices, licenses, and after-sales services. Service providers can use the virtual firewall technology to divide a purchased network security device into virtual firewalls to provide security functions for different enterprise networks. The enterprises share hardware resources, but their data flows are totally isolated. Virtual systems protect the enterprise networks at a lower cost, and bring rental income to the device owner.
- Network isolation for large and medium-sized enterprises: A large number of network devices are deployed on networks of large and medium-sized enterprises. Subnets are strictly divided and permissions are strictly controlled to protect core assets of the

enterprises. Though traditional firewalls can isolate networks by dividing security zones, the interface-based security zones may not meet the requirements on a complex network, and complex policy configurations are prone to errors. In addition, administrators of multiple networks have the same permission on the same device, which easily causes configuration conflicts. In contrast, the virtual firewall technology can divide a network into independently managed subnets, making network boundaries clearer and network management easier.

- Cloud computing: The cloud computing technology is used to store network resources and computing capabilities in the cloud. Users can access resources and services after they connect to the Internet. During this process, traffic isolation and security are important. The virtual firewall technology enables the USG, deployed at the egress of the cloud computing center or data center, to isolate user traffic and provide security capabilities.

To ensure that services in each virtual firewall are correctly forwarded, independently managed, and mutually isolated, the USGs virtualizes routes, security functions, and configurations.

- Route virtualization: Each virtual firewall maintains separate routing tables and session tables, independent and isolated from each other.
- Security function virtualization: Each virtual firewall has independent security policies and other security functions that apply only to packets of the virtual firewall.
- Configuration virtualization: Each virtual firewall has an independent virtual system administrator and configuration web UI. Administrators can manage only the virtual firewalls to which they belong.

Route, security function, and configuration virtualization simplifies the use of the virtual firewall function provided by the USG. The virtual firewall function enables the administrator and users of each virtual firewall to feel that they exclusively use a firewall device.

6.2.8 Interworking with the IDS

- Flexible networking model

  In addition to providing advanced anti-attack capability, the USG can work with the Intrusion Detective System (IDS) device that is deployed in bypass mode. The IDS device has rich attack behavior information.

  During the interworking with the IDS, the IDS informs the USG of automatically detected malicious attacks, intrusion, or other hidden security risks, and then the USG discards the attack packets or takes other actions accordingly. Interworking with the IDS isolates intrusion detection and attack processing, which fully exploits the advantages of each device and improves the system performance.

- Reliably proactive defense model

  By working with the IDS, the USG provides a highly reliable proactive defense model. This model provides a reliable security solution.

  The USG that has static security policies dynamically discovers hidden security risks through the IDS. Once discovering intrusions, the USG can dynamically modify security policies in real time to ensure the security of the entire network.

- Interworking protocols

  The USG provides protocols for interworking with IDS devices of different types.

6.2.9 Diversified Logs and Reports

Logs and reports are important for device management. Administrators can record and track events that occur during device operating only through logs and events. Based on logs and reports, administrators can find packet drop causes, locate and troubleshoot faults, identify occurred security events, and analyze bandwidth usage. Therefore, logs and reports enable administrators to understand the network status and adjust device configurations. The USG provides rich logs and reports for administrators.

The logs include:

- Traffic logs: provide visibility into traffic by user or application, which help understand bandwidth usage and whether security policies take effect.
- Treat logs: provide statistics on network threats (such as viruses, intrusion behaviors, DDoS attacks, Trojan horses, Botnets, and worms). Threat logs help you learn what threats have occurred or are occurring, and adjust the security policies for better attack defense.
- URL logs: provide alert and block statistics on requested URLs. You can view URL logs to check why access to some URLs is blocked or allowed.
- Content logs: provide statistics on uploaded and downloaded files and data, sent and received emails, and alert and block records on websites. Content logs help you learn risky user behaviors and why access to some URLs is blocked or allowed.
- Operate logs: record administrators' login, logout, and operations on devices. By analyzing operate logs, you can identify security vulnerabilities.
- System logs: record system events and hardware environments. System logs help you learn if the system has been functioning properly and perform troubleshooting when a fault occurs.
- User activity logs: provide visibility into users' online records (such as login time, online/lockout duration, and login IP and MAC addresses) and the actions users perform. User activity logs help you identify exceptions during user login and network access activities.
- Policy matching logs: record the policies that traffic matches. Policy matching logs help you locate faults.
- Mail filtering logs: provide visibility into the protocol types used by users to send and receive emails, size of a single attachment in an email, number of attachments in an email, and reasons why valid emails are blocked. Mail filtering logs help you locate faults in email services.
- Audit logs: provide visibility into user behaviors recorded by the audit function and how audit policies have been applied.

The reports include:

- Traffic reports: provide visibility into traffic trends and top flows in multiple dimensions
- Threat reports: display the threat count trend and top threats in multiple dimensions.
- URL reports: display the URL category hit/URL access count trend and top URL category hits/requested URLs.
- Policy matching reports: display the policy hit count trend and top policy hits. You can check policy hit reports to check if policy configurations are correct.

6.2.10 Flexible Device Management

- Diversified management measures

  - Local configurations and maintenance through the console port
  - Local or remote maintenance through Telnet
  - Maintenance and management through SSH, which provides advanced authentication functions to prevent attacks such as IP spoofing and plain-text password interception on insecure networks.
- SNMP-based terminal management: The USG supports SNMPv1/v2c/v3 and the Client/Server architecture. It can be managed by the network management system (NMS), for example, Huawei eSight.
- GUI configuration and management: The USG provides user-friendly Web Graphic User Interfaces (GUIs) for configuration and management. On GUIs, you can configure features, such as security zones, policies, NAT, ASPF, attack defense, data filtering, and traffic control and view statistics settings.

6.2.11 Test and Authentication Compliance

The USG is designed against international and national standards of China, Asia-Pacific, and Europe and meets hardware certification and network access requirements, such as Underwriter Laboratories Inc. (UL), Communate Europpene (CE), Electromagnetic Compatibility (EMC), and safety procedures.

7 Huawei Service

7.1 Service Concepts

1. Customer-oriented services

   Focus on the requirements and experience of the customer, improve the awareness and skills of service, and protect the network running of the customer with superior services to meet the security requirements of the customer.

2. Sophisticated services

   Constantly optimize service contents and provide professional, standard, and diversified services. Attach importance to service initiative and service personalization, build an excellent service brand, and maintain leadership in the industry.

7.2 Service Content

No.	Service	Supports from Other Parties	Documents
1	Preparations	Learn about the network conditions from the customer.	
2	Onsite service	Assistant personnel	Service implementation application Service implementation summary report
3	Test	Assistant personnel	Test report
4	Onsite training	Training venue and participants	Training summary report

7.3 Service System

Huawei has a three-tier service system for project implementation: the local office, technical support department, and R&D department.