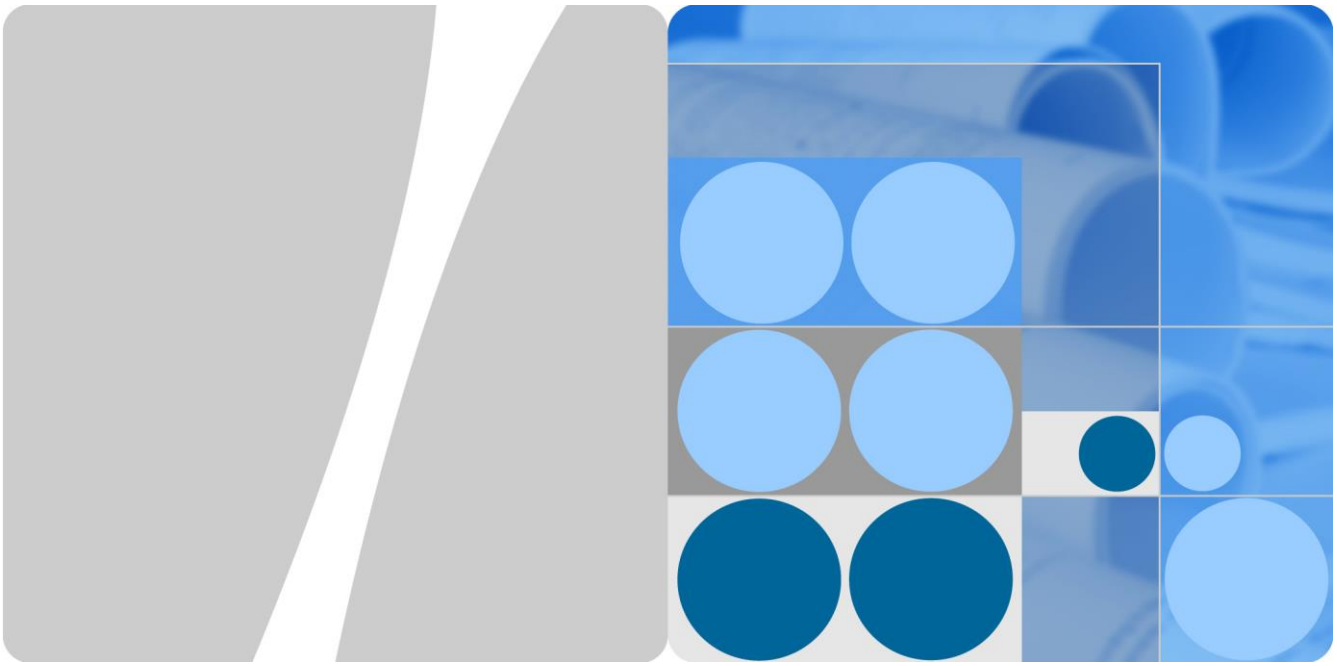


HUAWEI USG6000 Series Next-Generation Firewall Technical White Paper

Issue V1.1

Date 2014-03-12

HUAWEI TECHNOLOGIES CO., LTD.

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

Contents 2

1 Overview 5

1.1 Network Threats and Emergence of Next-Generation Firewalls (NGFWs) 5

1.2 NGFW Definition 5

1.3 Instructions on Using Firewalls 6

2 Technical Features of NGFWs 8

2.1 Reliability Design 8

2.2 Performance Model 9

2.3 Network Isolation 10

2.4 Access Control 10

2.5 Flow-based Stateful Inspection Technology 11

2.6 User-based Management and Control 11

2.7 Application-based Management and Control 11

2.8 Application-Layer Intrusion Prevention 11

2.9 Service Support 12

2.10 NAT 12

2.11 Attack Defense 12

2.12 Networking Adaptability 13

2.13 VPN Service 13

2.14 Management System 14

2.15 Log System 14

3 Technical Features of HUAWEI Secospace USG6000 Series 15

3.1 High Reliability Design 15

3.2 Flexible Security Zone Management 21

3.3 Security Policy Control 23

3.4 Stateful Inspection Based on Flow Sessions 24

3.5 ACTUAL Awareness 26

3.6 SmartPolicy 32

3.7 Advanced Virtual Firewall Technology 33

3.8 Service Support 34

3.9 NAT 36

3.10 Diversified Attack Defense Methods 38
3.11 High Networking Adaptability 41
3.12 Excellent VPN Functions 43
3.13 Application-Layer Security 46
3.14 Sound Maintenance and Management System 50
3.15 Comprehensive Log Report System 50
4 Typical Networking 55
4.1 Attack Defense 55
4.2 NAT 55
4.3 Hot Standby 56
4.4 VPN Applications Protected by IPSec 57
4.5 SSL VPN Application 59

HUAWEI Secospace USG6000 Series Technical White Paper

Keywords: NGFW, HUAWEI Secospace USG6000 series, network security, VPN, tunneling technology, L2TP, IPSec, IKE

Abstract: This document describes the technical features and working mechanisms of the Secospace USG6000 series and analyzes technical issues that you should pay attention to during firewall selection.

Acronym and Abbreviation	Full Spelling
VPN	Virtual Private Network
AAA	Authentication, Authorization, and Accounting
ASPF	Application Specific Packet Filter
DoS	Denial of Service
L2TP	Layer 2 Tunneling Protocol
IPSec	Internet Protocol Security
IKE	Internet Key Exchange
NGFW	Next Generation Firewall

1 Overview

1.1 Network Threats and Emergence of Next-Generation Firewalls (NGFWs)

With the rapid Internet development, increasing application quantity, and Web2.0 popularity, more bandwidth requirements and new application architectures (such as Web2.0) are changing the protocol use and data transmission methods. More and more applications use a few ports for transmission. New threats (such as worms, botnets, and other application-based attacks) continuously come into being. Security threats focus on seducing users into installing malicious programs that can evade the detection of security devices and software.

Traditional firewalls identify applications based on ports and protocols and perform attack detection and defense based on transport-layer characteristics. Security policies based on ports and protocols cannot provide sufficient defense capabilities in the scenarios where a large number of applications use a few ports or some applications use non-standard ports. The traditional firewalls cannot defend against application-based threats, such as worms and botnets.

Ever-changing business processes, enterprise deployment technologies, and threats bring about new requirements on network security. New security requirements have promoted the emergence of NGFWs.

1.2 NGFW Definition

Gartner defines a network firewall as an in-line security control that implements network security policy between networks of different trust levels in real time. Gartner has used the NGFW term to indicate the necessary evolution of a firewall to deal with changes in business processes, IT technologies, and network threats.

An NGFW has at least the following attributes:

1. Supports online "bump-in-the-wire" configuration without interrupt any network connection.

2. Checks network flows during transmission and implements security policies. The features are as follows:
   - Standard first-generation firewall capabilities, including packet filtering, Network Address Translation (NAT), stateful protocol inspection, and VPN
   - Integrated network intrusion detection: The NGFW supports vulnerability-specific and threat-specific feature codes. The interaction effect of the IPS and firewall is greater than the sum of two separate parts. For example, an NGFW automatically binds conditions to apply firewall rules to prevent an address from loading malicious traffic to the IPS, but does not require administrators to deploy the solution cross consoles. The NGFW has integrated powerful IPS engines and feature codes.
   - Application awareness and full-stack visibility: The NGFW identifies applications and implements network security policies that are independent from ports, protocols, and services. For example, the NGFW allows the use of Skype, but disables file sharing in Skype or always blocks the GoToMyPC function.
   - Excellent firewall intelligence: The NGFW collects incoming information, helps administrators make better decisions, and optimizes the deny rule database. For example, the NGFW binds the deny action to user identities or set up the address blacklist and whitelist.

1.3 Instructions on Using Firewalls

Firewalls are deployed at convergence points on the entire network. If traffic of the protected network has bypassed a firewall, the security defense function of the firewall does not take effect. Therefore, when you use a firewall, ensure that all traffic of the protected network passes through the firewall.

By default, firewall rules deny all access requests. After connecting a firewall to the network, you must configure security policies based on actual conditions. Policy effectiveness, diversity, and flexibility are important indexes to evaluate a firewall. In the complex network environment that has massive rules, you must consider the rule capacity and forwarding performance of the firewall.

Firewall security is also an important criterion. Security performance of a firewall depends on the operating system and hardware platform. The secure operating system guarantees the software security of the firewall, and the dedicated hardware platform enables the firewall to run stably for a long time. Firewall is a basic network device and must run for a long time without any interruption. Therefore, hardware reliability is critical.

Before using a firewall, you must determine issues to be resolved on the live network and select the firewall that meets requirements on performance and functionality. The firewall performance and functionality must be balanced. However, you must pay special attention to performance indexes, because they are critical to the actual operating. If the firewall is poor in performance, network congestions and failures frequently occur. Such a network is insecure. Performance indexes reflect the available firewall capabilities and the costs

that an enterprise uses the firewall. The enterprise cannot afford too high costs. If a firewall causes long delays, users also experience great losses.

Mainstream firewalls are the stateful inspection ones that are sensitive to service applications. Protocols of multimedia services (such as audio and video services) are complex. If the protocol status is improperly processed, services may be interrupted or unnecessary ports must be opened to ensure service continuity. However, the opening of unnecessary ports degrades security. Therefore, you must consider the service adaptability of stateful firewalls, so that the firewalls do not adversely affect network services.

2 Technical Features of NGFWs

2.1 Reliability Design

A firewall is the key network device deployed at the network egress. The firewall requires high reliability because of its location and functions.

The high reliability is implemented on the basis of the following technologies:

- Reliable hardware design. Different from personal or household systems, network devices are required to work 24 hours without any interruptions. This is demanding for hardware components, such as the main board, CPU, fans, and cards. To ensure uninterrupted operating for a long time, the firewall must have an excellent hardware structure.
- Hot standby technology. To ensure the reliable operating at a key location, the firewall must provide hot standby. Hot standby requires two independent devices of the same model to work together to provide a more reliable working environment. Two devices deployed in hot standby mode can work in either of the following modes. Only one of the two devices is working, and the other device takes over services if one device fails. Two devices are working. If one device fails, the other device takes over all services.
- Link backup technology. Link backup prevents physical link faults from interrupting services. Link backup is implemented as follows: Two links are used to carry services. When both links are normal, service traffic may select links in load balancing mode. When one link fails, service traffic of that link is automatically switched to the other link. To implement link backup, the firewall must support various routing protocols and provide route management functions. The route-based link backup technology can well suit different scenarios and provide more reliable services by implementing the mutual backup of links.
- Hot backup technology. Hot backup means that services are not affected during the device or link switchover when a fault occurs. If the backup occurs when services are interrupted due to a fault, such backup mechanism is called cold or warm backup. In most documents, hot backup, warm backup, and cold backup are not strictly distinguished. Many vendors advertise their hot backup concepts, but most their backup mechanisms are cold or warm backup. More dynamic information has more complex hot backup mechanism. Each firewall maintains large amounts of rule and connection data. The hot backup mechanism of firewalls is complex. Therefore, you must distinguish hot backup from cold backup when choosing firewall backup technologies.

The reliability design of firewalls reflects comprehensive considerations. Firewalls are important network devices that have demanding requirements on reliability. Therefore, you must consider the reliability design during firewall selection.

2.2 Performance Model

This section describes the indexes that you must pay attention to when measuring firewall performance.

Throughput is a key index to evaluate firewall performance in the industry. Throughput refers to the total traffic that a firewall can forward with the best effort in the case of large packets, in bit per second (bit/s). However, the throughput does not reflect the actual working capabilities of the firewall, and using the throughput as the only performance index is one-sided.

In addition to the throughput, you must consider the following indexes:

1. Small-packet forwarding capability

In the industry, large packets of 1 KB to 1.5 KB are used to measure the processing capability of a firewall. Since network traffic mainly comprises 200-byte packets, the capability of forwarding small packets must be assessed. This performance reflects the actual forwarding capacity of the firewall on the live network.

2. Impacts on forwarding efficiency by rule quantity

A firewall is generally running with a large number of rules. The implementation of rules and services may affect the forwarding performance. Therefore, you must pay attention to the forwarding efficiency of a firewall in the scenarios where massive rules and services exist to avoid performance deterioration.

3. Number of new connections per second

The index is the number of TCP connections that can be established on a firewall per second. Connections are dynamically established on the basis the communication status of two parties. Each session must establish a connection on the firewall before data exchange. If the firewall has a low connection setup rate, the communication delay is long on clients. The larger the specification, the higher the forwarding rate, the stronger the status backup capability, and the more powerful the attack defense capability. The number of new connections per second is an important index to measure firewall functionality. If this index is low, the firewall cannot present excellent performance in actual network environments and even cannot work under DoS attacks.

4. Number of concurrent connections

A firewall processes packets based on connections. The index the maximum number of connections supported by the firewall. Each connection is TCP/UDP access.

5. Delay

Delay is the time for transmitting data in the case of no packet loss. The delay must be as short as possible. The delay is critical in the scenarios that require high timeliness, such as voice and video services. The long delay of a firewall results in harmonic distortion and service interruption. Therefore, the delay is a key index of firewall performance.

During firewall selection, you may consider other indexes based on actual requirements. You must note that a firewall is a data communication device to process complex services and the performance indexes are much more in amount than any traditional data communication device. The performance indexes of a firewall also reflect the comprehensive indexes of the firewall, such as the software design and hardware design. Therefore, the performance indexes are important during firewall selection.

2.3 Network Isolation

The essential function of a firewall is to isolate network areas. The firewall isolates the logical networks of common areas and key areas to avoid the spread of insecure factors. Network isolation is an important feature in the firewall technology system. Security policies can be effectively implemented only after you have divided network areas properly. To check whether network isolation is correct, examine the following aspects:

The network isolation system of a firewall has a clear logic structure to make the firewall meet requirements in different scenarios. For example, a firewall must have a Demilitarized Zone (DMZ).

Network areas must interwork with physical interfaces during network isolation, and the division of network areas cannot rely on physical interfaces only. If only physical interfaces are used for network isolation, requirements on flexible implementation cannot be met. Network isolation is a logic concept and must be flexibly implemented to meet service requirements.

When you isolate networks, you must consider the implementation of virtual interfaces, such as the tunnel, VPN, and VLAN interfaces. Network services are ever-changing. VPN isolation and VLAN isolation are widely applied on networks. Domain isolation must apply different virtual interfaces with services such as VPNs and VLANs.

You must consider the security of a firewall itself. The firewall is a control point of network isolation and must be secure. The firewall security is the basis of network security. You must also consider the access to a firewall from the network areas that are isolated by the firewall.

2.4 Access Control

The access control function of a firewall is important and applies Access Control Lists (ACLs). Each ACL defines a series of rules based on packet characteristics to control the packets that pass through the firewall. In some scenarios, a large number of rules are specified on the firewall. Therefore, the rule capacity is a key index of evaluating firewall performance and functionality.

2.5 Flow-based Stateful Inspection Technology

The ACL-based IP packet filtering technology is widely used in access control. This technology is simple and reliable, but lacks flexibility. For the communication using multi-channel protocols such FTP, the firewall is difficult to configure. FTP includes a TCP control channel with predefined ports and a TCP data channel that is dynamically negotiated. You cannot obtain the port number of the data channel when configuring security policies on a common firewall. Therefore, the ingress of the data channel cannot be determined. The stateful inspection technology can resolve such an issue. By detecting the status of data packets, the firewall dynamically discovers ports to be opened to determine the packets that are allowed to pass through the firewall during the communication process.

The flow-based stateful inspection technology provides high forwarding performance. ACL-based packet filtering detects packets one by one. As a result, the firewall performance is degraded when there are massive filtering rules. Flow-based stateful inspection, however, determines whether a packet is allowed to pass through the firewall based on flow information. Such processing improves the forwarding performance.

Mainstream firewalls mainly use the stateful inspection technology. You are advised to consider a stateful firewall first.

2.6 User-based Management and Control

An NGFW performs security policy control by IP address and user identity.

The NGFW must monitor the user logins and logouts, and control user permissions and assign bandwidths by user or user group.

2.7 Application-based Management and Control

An NGFW performs security policy control by port as well as in-depth application identification by protocol and carries out application-based management and control according to the identification results.

The NGFW must support continuous updates of pattern files (used for identifying applications) to prevent employees from evading firewall monitoring by updating applications or using new applications.

2.8 Application-Layer Intrusion Prevention

An NGFW defends against traditional network-layer attacks as well as application-layer threats. The NGFW must integrate application identification and decoding capabilities, identify worms, botnets, and other application-based attacks, detect the contents transmitted by applications, and perform application-layer content filtering to prevent information leaks and illegitimate transmission.

2.9 Service Support

A firewall is deployed at the control point of network services. An important measure of the network security solution is to find a balance between openness and security. Because of technical features, the firewall may affect some services when being deployed on a network. To meet the requirements on service expansion, you must consider the service support capabilities of a firewall as follows:

- Supports diversified services using flow-based stateful inspection. With the growth of network resources and bandwidths, more and more services based on broadband applications come into being. You must ensure that the flow-based stateful inspection technology supports various services.
- Supports all multimedia services, such as voice and video services based on H.323, SIP, and RTSP, that account for a large proportion of broadband services.
- Supports powerful Network Address Translation (NAT) functions. Public IPv4 addresses are in great shortage. Therefore, NAT is a must to provide services. Because a firewall is deployed at a key position, configuring NAT on the firewall is one of the most common services. In addition, NAT hides the intranet structure, which effectively ensures intranet security.
- Supports necessary multicast services.
- Supports various Quality of Service (QoS) measures.

2.10 NAT

With the rapid development of the Internet, public IPv4 addresses are exhausted. Before IPv6 is applied, NAT is a major technology that resolves this problem.

NAT is proposed to resolve public IP address shortage to enable intranet users to access the Internet. NAT protects privacy of the intranet and provides Internet users with services such as WWW, FTP, Telnet, SMTP, and POP3. NAT functions include forward NAT and reverse NAT. The forward NAT has two forms: NAT and Port Address Translation (PAT).

Because of the deployment position and technical features of a firewall, NAT services provided by the firewall are suitable. Therefore, providing comprehensive NAT services is a necessary feature of the firewall.

2.11 Attack Defense

Attack defense is a key firewall function. The firewall must have the following attack defense capabilities:

- Defends against DoS attacks.
- Defends against malformed packet attacks and intelligently identifies attack packets.

- Defends against scanning and sniffing attacks.
- Provides comprehensive and diversified attack defense methods. DoS attacks are launched using different means. Therefore, the firewall must provide diversified methods to defend against these DoS attacks.
- Has excellent processing capabilities. An important feature of DoS attacks is the sudden increase of network traffic. If a firewall does not have excellent processing capabilities, the firewall itself becomes a bottleneck when processing the traffic of DoS attacks. Defending against the DoS attacks is impossible. A DoS attack is to make the target network paralyzed. If network congestion occurs on a key device, the attack objective is achieved.
- Has accurate attack identification capabilities. When processing traffic of DoS attacks, many firewalls only ensure that the traffic passing through them falls into an acceptable range, but cannot accurately identify attack packets. Such processing ensures the normal network traffic and server operating, but blocks legitimate users from accessing the Internet. The network plane is normal, but services of the legitimate users are denied. Therefore, the firewalls still fail to defend against DoS attacks.

2.12 Networking Adaptability

Because of the complex network deployment, the firewall must provide excellent networking adaptability for constructing service networks flexibly. Excellent networking adaptability includes the following aspects:

- Supports abundant interfaces to meet the requirements on networking adaptability at the physical connection layer.
- Supports routing protocols. Most firewalls support static routing protocols, but not dynamic routing protocols. However, supporting dynamic routing protocols can effectively improve the networking adaptability of a firewall.
- Supports the transparent mode. The transparent mode helps a firewall to work in Layer 2 mode. Therefore, when you add the firewall to a network, the existing network topology is not affected.
- Supports various virtual interfaces, such as VLAN sub-interfaces and tunnel interfaces. A firewall provides limited physical interfaces. To adapt to more complex networking schemes, the firewall must support various virtual interfaces.

2.13 VPN Service

Firewalls are deployed at the network border of an enterprise. The firewalls, with powerful control capabilities, can provide VPN services to ensure the communication between the headquarters and branch offices.

IP VPN is a common VPN technology, including the IPSec VPN, L2TP VPN, and GRE VPN. The IP VPN technology, applied at network borders, enables remote users and mobile users to securely and efficiently access the intranet.

The firewall provides the following VPN services:

- Provides VPN services to enable the communication among branch offices. IPSec tunnels are used to provide secure and reliable VPN services.
- Provides VPN access services for mobile office employees. The firewall must support Layer 2 VPN protocols. The widely applied Layer 2 VPN protocol is L2TP. L2TP provides VPN services and enables employees on the move to securely access the intranet using accounts and passwords.
- Provides efficient encryption services.
- Supports comprehensive VPN protocols, including GRE, IPSec, and L2TP.
- Strictly complies with RFC and protocol standards to interwork with the VPN devices of other vendors.

2.14 Management System

The firewall management system must have the following features:

- User-friendly man-machine interface. Users can manage a firewall through diversified methods.
- Easy upgrade methods, such as online upgrade using hot patches
- Graphical management that allows convenient configuration and policy management
- Remote maintenance and monitoring
- Secure and reliable remote logins, such as, the remote login using SSH

2.15 Log System

System logs enable after-the-event audit. A firewall logs various operations and attacks and provides the log query and filtering means to facilitate search and analysis.

3 Technical Features of HUAWEI Secospace USG6000 Series

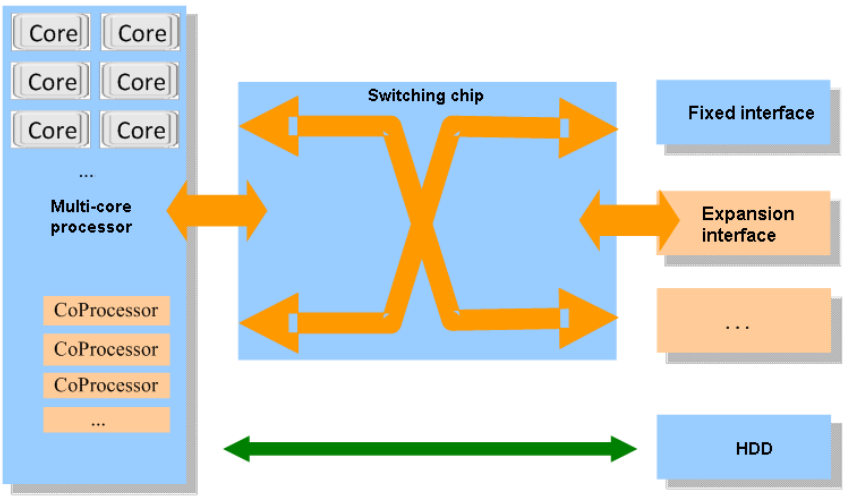
3.1 High Reliability Design

HUAWEI Secospace USG6000 series uses the carrier-class hardware system and dedicated software system (Huawei-proprietary VRP) to provide high security and reliability and effectively resolve the conflicts between high performance and complex service processing. With the highly reliable hardware design, robust software system, hot standby, link backup, and hot backup, the USG6000 series ensures high network reliability.

NG_Security Hardware Platform of NGFW

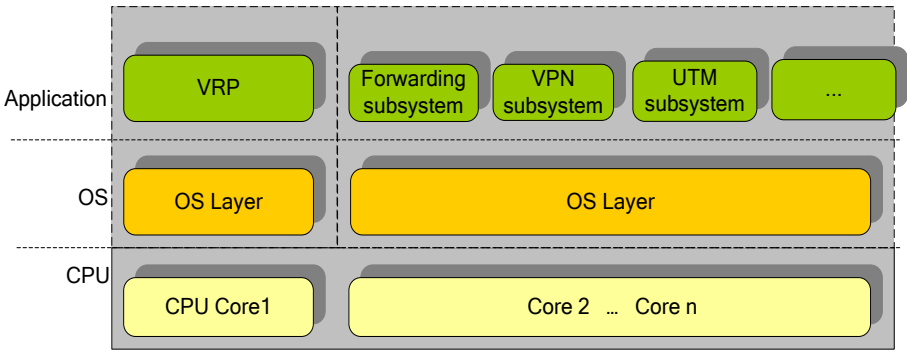
NG_Security hardware platform is a next-generation high-performance hardware platform developed by Huawei for security products. This platform, with a "Multi-core MIPS+Hardware co-processor acceleration+High-speed Switch Fabric" architecture, uses a high-speed bus to implement the communications between the multi-core CPU and the service processing and interface expansion modules. The redundancy design of the platform improves hardware reliability. In addition, the NG_Security hardware platform has enhanced performance and functionality and expands storage to meet requirements on the local storage of security device logs.

Figure 3-1 Huawei NG_Security hardware architecture



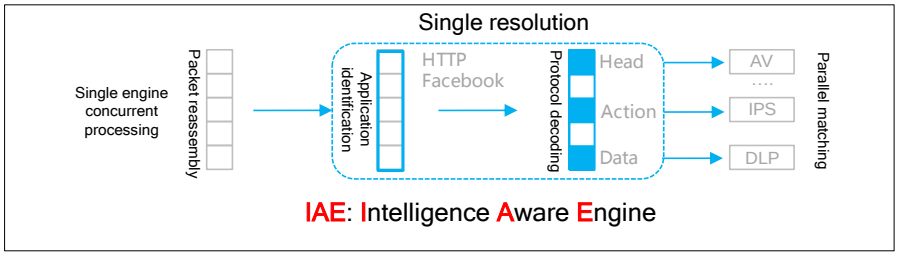
- Multi-core MIPS CPU

Huawei NG_Security hardware platform uses a 64-bit multi-core MIPS architecture that has high performance and is based on the regularly encoded instruction set of a fixed length. The MIPS architecture provides streamlined instruction sets, hierarchical design of the instruction and high-speed data cache, concurrent multi-level flow lines, and dedicated high-speed interfaces and DMA capabilities for traffic throughput, and incorporates Huawei carrier-class embedded real-time operating system to ensure the high performance of the NGFW platform.



The NG_Security hardware platform can be expanded with a CPU processing unit to implement "1+1" CPU capabilities. Each CPU is a multi-core MIPS processor. Such expansion doubles hardware processing capabilities.

Figure 3-2 Huawei NG_Security software platform



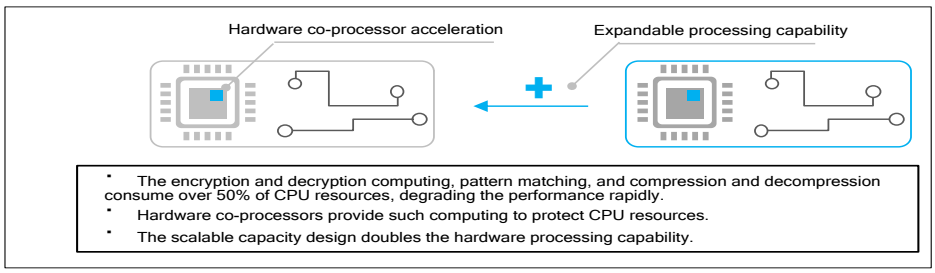
The architecture of the Intelligence Aware Engine (IAE) on the USG6000 series is different from that of traditional threat detection engines. The attack detection engine of a conventional firewall matches each packet with the attack signature database. Attacks can easily evade such detection. The IAE reassembles packets based on sessions, parses protocols, and matches signatures for a more accurate detection of protocol-specific attacks. During attack detection, the IAE parses each packet only once over the multi-core CPU architecture and can perform multiple security inspection tasks at the same time. The hardware acceleration module identifies applications and matches signatures at a high speed. If all signatures for an attack are met, the IAE takes an appropriate action according to the configured policy. If the signatures are not met, the IAE automatically adjusts the tracing status to ensure the high-speed forwarding of secure traffic. This architecture ensures the minimum compromise of the overall performance with multiple security services enabled.

The IAE uses a multi-core hardware platform for concurrent service processing. In addition, the IAE uses the hardware acceleration technology for application identification and signature matching, greatly improving attack detection efficiency.

- Hardware co-processor acceleration

Huawei NG_Security hardware platform has integrated the IPSec and SSL encryption and decryption, compression and decompression, pattern matching, and hard disk RAID hardware co-processors. These co-processors processes the services that may degrade CPU performance, such as encryption and decryption, compression and decompression, and pattern matching to reduce the consumption of CPU resources.

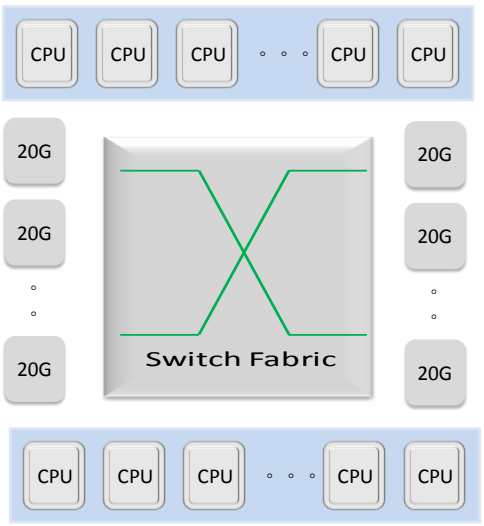
Figure 3-3 Huawei NG_Security co-processor and CPU expansion capabilities



- High-speed Switch Fabric

Huawei NG_Security hardware platform uses a 480 Gbit/s switching chip for the communications among the multi-core CPU, service processing module, and interface expansion module. Its high-speed switching bus provides sufficient bandwidths for all modules and ensures the smooth switching.

Figure 3-4 Huawei NG_Security software platform



- Storage module

Huawei NG_Security hardware platform supports the 300 GB high-speed SAS hard disk to store real-time logs and reports.

Two hard disks work in RAID1 mode to back up user data.

The hot swap design of hard disks enables capacity expansion and upgrade.

- Scalability

1. The USG6000 series uses the flexible and scalable architecture to double security performance by adding more SPUs for different application scenarios. The combination of the intelligent awareness engine and the elastic hardware structure enable the USG6000 series to deliver 10-Gigabit level threat prevention performance, meeting the security protection requirements of large enterprise data centers.
2. The NGFW supports multiple slots for high-density expansion interface cards and diversified interface cards that provide the GE electrical and optical ports and 10GE ports. You can flexibly improve hardware forwarding capabilities and device performance according to actual conditions.
3. Based on the virtual system function of the USG6000 series, you can divide a physical device into multiple virtual devices that are independent and locally isolated to implement system-level expansion and meet the requirements of device leasing and cloud computing.
4. Hard disks are optional. You can choose hard disks as required.

The previous scalability features enable customers to configure only required modules in the initial phase and expand capacities when necessary to maximize customer investments.

- High reliability

1. Power supplies provide 1+1 redundancy, and hard disks work in RAID1 mode. When one power supply or hard disk is faulty, the other one takes over all the services. The hardware design ensures service continuity.
2. Fault detection: The system monitors the working statuses of the integrated device and key components on SPUs and LPUs and generates alarms (such as the fan failure, power failure, and over temperature alarms) when an anomaly is detected.
3. Hot standby: The comprehensive hot standby mechanism ensures high availability. When an NGFW is faulty, services are smoothly switched to the other NGFW without affecting user services. Hot standby implements real-time data backup for key configurations and connection entries to ensure that firewall performance is not affected by the switchover. You can also manually back up data in batches.
4. Hardware bypass: The built-in bypass card is supported. If the NGFW is faulty, traffic is bypassed to ensure service continuity.

- Energy-saving and eco-friendly design

Dynamic power consumption management: The NGFW has an architecture that uses low power consumption components and high efficiency power supplies to reduce power consumption. In addition, system software dynamically controls power consumption based on the device operating, function enabling, port connection, and temperature statuses, for example, dynamically closing idle ports and functional units and adjusting fan speeds.

Intelligent heat dissipation: The NGFW uses PWM speed adjustment fans and reduces power consumption by 70% using the refined speed adjustment and area-specific heat dissipation technologies. The technologies also reduce noises.

Eco-friendly manufacturing process: The design and production of the NGFW strictly comply with RoHS and WEEE laws and regulations, without any toxic substances. The design allows product disassembly and has high recyclability. Recyclable materials are widely used, and the product recycle ratio is above 90%. The packing design complies with the EU requirements 94/62/EC. Eco-friendly and recyclable materials are used, and the types, quantity, and weight of required materials are reduced.

Robust Software System

The USG6000 series uses Huawei-proprietary VRP operating system as its core component. Therefore, the USG6000 series itself can prevent unreliable elements, such as security vulnerabilities in universal operating systems, viruses, and attacks.

The VRP operating system is a dedicated platform for data communications. Its software architecture is customized for data communications devices and has taken the development of communications technologies into consideration. The USG6000 series not only ensures reliable and secure operating, but can also be

expanded for the further development of security technologies. All these factors endow the technology advance of the USG6000 series.

Hot Standby

Hot standby of the USG6000 series means that two independent devices of the same model work simultaneously to provide a more reliable operating environment. The USG6000 series can work in either of the following modes:

- Only one of the two devices is working. If one device fails, the other device takes over its services.
- Both devices are working to implement load balancing. If one device fails, the other device automatically takes over all tasks.

Hot Backup

Hot backup means that services are not affected during the device or link switchover when a fault occurs. If the backup occurs when services are interrupted due to a fault, such backup mechanism is called cold backup. The USG6000 series implements hot backup on firewall configuration and dynamic traffic, including filtering rules, connections, dynamic routing information, and state machines of application-layer protocols in status check. The more dynamic information is, the more complex the hot backup mechanism is.

Link Backup

Link backup prevents physical link faults from interrupting services. The USG6000 series provides two links to carry services. When the two links are normal, traffic may select both links in load balancing. When one link fails, traffic of that link automatically fails over to the other link. The USG6000 series dynamically adjusts routing protocols during the switchover. Therefore, the route-based link backup technology of the USG6000 series can well suit different scenarios and provide more reliable services based on the mutual backup of links.

BFD

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

As an independent hello protocol, BFD implements low-overhead and rapid fault detection. By interworking with upper-layer protocols, BFD enables them to rapidly identify and recover from faults. BFD can interwork with OSPF, static routing, Fast ReRoute (FRR), policy-based routing (PBR), and DHCP to rapidly identify link faults.

Advantages of Huawei Firewalls in Reliability

The hot standby mechanism of HUAWEI Secospace USG6000 series has the following advantages:

- Since Huawei USG6000 series has expanded the Virtual Router Redundancy Protocol (VRRP) to the VRRP Group Management Protocol

(VGMP) to control and guarantee the consistency of VRRP, it has abundant advantages in LAN application. Because VRRP reliability technology is proved to be stable and reliable in LANs and can be transparent to users in LANs, the hot standby solution of the USG6000 series has distinct advantages in LANs or the access points of intranets.

- The hot standby technology of the USG6000 series is based on HRP, which is a quick and efficient hot standby technology developed by Huawei. Through the hot standby technology, multiple HRP backup channels with different priorities can be configured according to live-network traffic. Due to the quick backup of the session table, users' applications are not interrupted during the active/standby switchover caused by firewall faults.
- The hot standby technology of the USG6000 series supports preemption, which is important for the networking in which devices back up each other to share traffic. Since all the traffic is switched over to one firewall once the other is faulty, a practical mechanism is needed to ensure that the traffic can smoothly switch back to the original faulty firewall when it recovers. The hot standby technology supporting preemption guarantees the smooth switchover and therefore ensures the reliable operating of the devices in mutual backup networking.
- The USG6000 series supports OSPF +VRRP hybrid networking. When a fault occurs, the firewalls dynamically adjust OSPF parameters so that the traffic can be quickly switched over to the other device. In this way, traffic can be smoothly switched back in the event of failure recovery and reliable operating of the backup networking is guaranteed.
- The USG6000 series supports the hot standby solution in hybrid mode, ensuring that the service interfaces of the firewalls can back up traffic and work in transparent mode without any influence on the existing network topology, so that users' services are not interrupted during the switchover caused by firewall faults.
- The USG6000 series supports diversified networking modes, and each mode can provide the full redundancy of devices and links, which ensures the stable operating of the high reliability network.

3.2 Flexible Security Zone Management

Isolation by Security Zone

Based on security zones, the security isolation design of the USG6000 series provides an excellent management model for users in the actual application of firewalls.

The core function of a firewall is network isolation, and the network isolation technology does not rely only on interfaces in network division. Network topologies vary with actual conditions. Network isolation based on fixed interfaces cannot meet requirements on the live network.

The USG6000 series provides an isolation model based on security zones. Each security zone can be added to any interface according to actual conditions, not affected by the network topology.

Manageable Security Zones

Many firewalls in the industry provide independent Trust zones, Untrust zones, and DMZs. Such protection model meets most networking requirements. In some scenarios that have demanding requirements on security policies, this protection model cannot meet the requirements.

The USG6000 series provides four default security zones: Trust, Untrust, DMZ, and Local. It has added the Local zone that defines packets destined for the firewall itself, which enhances security protection for the firewall itself. For example, by controlling the packets in the Local zone, the USG6000 series easily prevents the access initiated from insecure zones using Telnet or FTP.

The USG6000 series also supports user-defined security zones. Independent interfaces can be added to each security zone.

Policy Control by Security Zone

The USG6000 series supports the design of security policy groups for the access between security zones. Each security policy group supports several independent rules. Such a rule system enables easy management of firewall policies and facilitates independent management over logical security zones.

The policy control model based on security zones can clearly define the access from the Trust zone to the Untrust zone and from the DMZ to the Untrust zone. The model enables the network isolation function of the USG6000 series to provide excellent management capabilities.

Comprehensive Service Capability

Security zone management of a firewall covers all physical interfaces, subinterfaces, Loop Back interfaces, tunnel interfaces, dial-up logic interfaces, and virtual-template interfaces. The policies of security zone management support all types of services on the firewall. Independent security zone management of the USG6000 series isolates network areas accessing through VLANs.

The USG6000 series supports management over the Local zone. You can easily define policies to allow external users' access to the USG6000 series itself. By defining these policies, you can flexibly set the management rules of the USG6000 series. For example, you can permit users in a security zone to log in to a firewall and interfaces in a security zone to communicate with the firewall. Such an operation manages the firewall itself and distinguishes firewall management policies from service flow management policies, helping you define clear security policies.

The security policies of the USG6000 series can be defined on the basis of security zones in a centralized manner. For example, the levels of defense against DoS attacks may vary with security areas. Through the support of services, the policies and control modes of the USG6000 series can cooperate well with the security zones. In this way, the USG6000 series provides security defense and policy management at the system level, therefore facilitating management and implementation of services and policies, and the security defense system becomes clearer.

3.3 Security Policy Control

Flexible Rule Setting

The USG6000 series supports flexible rule settings based on packet characteristics. It provides the following functions:

- Sets rules based on the protocol number of packets.
- Sets rules based on the source and destination addresses of packets.
- Uses a wildcard character to define an address range to specify hosts of the address range.
- Sets a source or destination port for UDP or TCP.
- Sets a port range for the source and destination ports using the methods such as greater than, equal to, between, or not equal to.
- Defines the type and code of ICMP packets and configures a rule for each type of ICMP packets.
- Sets flexible rules based on the ToS field of IP packets.
- Sets filtering rules based on the user groups and names of Internet access users.
- Sets filtering rules based on application categories and protocols.
- Sets filtering rules based on locations.

Rule Management by Time Segment

ACL policies of the USG6000 series can be managed by time segment. You can configure absolute time segments or periodic time segments. You can easily configure time-specific policies on the USG6000 series using time segments. For example, forbid the use of Skype in working hours and allow the use of them in non-working hours.

ACL-based policies can be configured on the basis of time segments. For example, NAT services define policies based on ACLs. Time segments can be used to provide more flexible NAT services. QoS defines data flows based on ACLs. Time segments can also be used to configure time-specific QoS policies.

High-Speed Policy Matching

Policy matching may affect firewall efficiency because each policy consists of many rules.

The USG6000 series uses Huawei-proprietary ACL quick search and matching algorithm that enables the USG6000 series to maintain highly efficient forwarding when a large number rules exist. When searching thousands of ACL rules, the system performance is almost not affected and the processing speed remains unchanged. Therefore, high-speed policy matching of the USG6000 series improves the overall system performance.

IP-MAC Binding

According to user configurations, you can bind MAC addresses to IP addresses on the USG6000 series. If packets from an IP address do not match the bound MAC address, the USG6000 series discards the packets. The USG6000 series sends packets that are destined for an IP address to the bound MAC address to prevent IP spoofing attacks.

Dynamic Policy Management — Blacklist

The USG6000 series blacklists the source IP addresses of untrusted packets and discards all the packets of the blacklisted users, therefore effectively preventing the attacks from malicious hosts.

The USG6000 series provides the following blacklist maintenance methods:

- Manually adding entries to the blacklist to implement proactive defense
- Automatically adding blacklist entries through attack defense to implement intelligent protection
- Interworking with the whitelist to allow the blacklisted host to access some network resources. For example, users are allowed to access the Internet using a host even if the host is blacklisted.

Blacklist is a dynamic policy technology and belongs to the response system. The USG6000 series can identify some attack behaviors during dynamic running. It controls the traffic of these illegitimate users through the blacklist dynamic response system to protect the entire system.

3.4 Stateful Inspection Based on Flow Sessions

Kernel Technology Based on Session Management

The USG6000 series is an advanced stateful firewall based on flow sessions and has integrated powerful kernel technology based on session management. It provides two core processing units: first-packet processing unit and session management unit. They rely on independent acceleration systems in terms of management. Such processing has the following advantages:

- The first-packet processing unit avoids bottleneck of the USG6000 series in the processing of the first packet. It enables the USG6000 series to provide outstanding performance of new connections per second and maintain excellent processing performance on the live network.
- The session management unit equips the USG6000 series with an extraordinary forwarding acceleration system, delivering high forwarding performance. The forwarding performance of the USG6000 series for subsequent packets relies on the independent acceleration system to achieve accelerated packet forwarding, so that the USG6000 series delivers high forwarding performance besides the brilliant processing of new connections per second.
- The connection management of the USG6000 series can be at a fine granularity. On most firewalls, you can configure policies only over TCP

or UDP in terms of connection management. On the USG6000 series, you can configure management policies by service type. For example, you can configure management policies for Telnet and HTTP.

- The service processing of a firewall is based on session management, so that the firewall can support abundant services. For example, the USG6000 series supports service features such as PBR and QoS. These features can be managed on the flow basis. With the flow-based forwarding and stateful inspection technologies, the USG6000 series provides diversified flow-based services to meet requirements in various operating environments.

In-Depth Inspection

The USG6000 series provides ASPF that is an advanced communication filtering technology to check application-layer protocol information and monitor connection-based application-layer protocol status. The USG6000 series, relying on access control based on packet content, detects and defends against some application-layer attacks. It also detects FTP commands, SMTP commands, HTTP Java, and ActiveX controls.

ASPF provides in-depth inspection based on session management. The ASPF technology uses information in the session management module to maintain session access rules. It saves session status information that cannot be saved by static access list rules in the session management module. The session status information can be used to intelligently permit or deny packets. When a session terminates, the ASPF session management module removes the session information from the session table and closes the session on the firewall.

ASPF intelligently detects the TCP three-way handshake and the connection removal handshake. Stateful inspection on the handshake and connection removal ensures that a TCP access can normally proceed and the packets of incomplete TCP handshake connections are denied directly.

Advantages of Stateful Inspection

ACL-based IP packet filtering is applied in common scenarios. This technology is simple and inflexible. In many complex scenarios, common packet filtering is unable to protect networks. For example, configuring packet filtering rules is difficult for multi-channel protocols such as FTP. FTP includes a TCP control channel with predefined ports and a TCP data channel that is dynamically negotiated. You cannot obtain the port number of the data channel when configuring security policies on a packet filtering firewall. Therefore, the ingress of the data channel cannot be determined, and security policies cannot be accurately configured. The ASPF technology resolves this problem. It detects application-layer packet information and dynamically creates and deletes temporary rules based on packet content to permit certain packets.

ASPF enables the USG6000 series to support multiple data connections over one control channel. It facilitates security policy configuration in complex application scenarios. 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 dynamically select ports to transmit data. Port selection is unpredictable. An

application may use more than one port at a time. Therefore, packet filtering firewall prevents only single-channel transmission of applications and blocks the applications using fixed ports, which brings about many security risks. ASPF listens to the port used by each connection of an application, opens an appropriate path to permit data of a session, and closes this path at the end of the session. In this way, the USG6000 series effectively implements access control over the applications using dynamic ports.

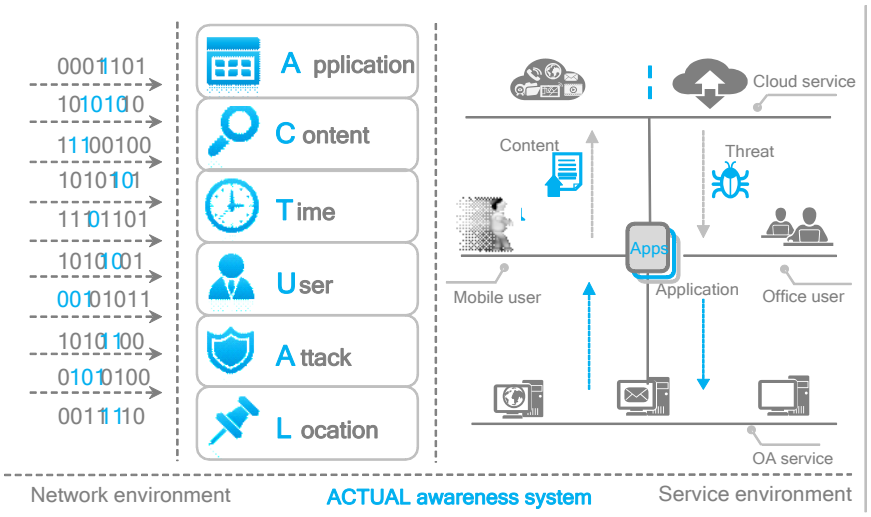
When a packet reaches the USG6000 series, ASPF matches the packet with access rules. If a match is found, the packet can pass through the USG6000 series. Otherwise, the packet is discarded. If a packet is used to open a control or data connection, ASPF dynamically modifies access rules. The returned packets can pass through the USG6000 series only after matching an access rule. When processing the returned packets, ASPF also updates the status information table. After a connection is closed or timed out, ASPF deletes the status information table of the connection, preventing unauthorized packets from passing through the USG6000 series.

3.5 ACTUAL Awareness

Networks are evolving into next-generation networks that feature explosive information growth, borderless network, mobile Internet, and Web2.0. Cybercriminals can easily penetrate a traditional firewall that uses quintuple ACLs by spoofing or using Trojan horses, malware, or botnets. Under this background, the USG6000 series of Huawei provides an "ACTUAL" (Application, Content, Time, User, Attack, and Location) awareness technology to accurately control network traffic in a refined manner, defend against security threats, and ensure intranet security.

Definition

ACTUAL awareness is the capability of identifying network traffic by application, content, time, user, attack, and location. Based on the ACTUAL awareness results, you can configure security policies such as the filtering, route selection, traffic control, and NAT policies.



As shown in the previous figure, network traffic is complex. The administrator of a traditional firewall cannot accurately analyze or obtain real service traffic types, and cannot apply security policies to control network traffic. ACTUAL awareness of the USG6000 series analyzes the traffic of complex network environments, provides the administrator visibility into statistics on traffic by application, content, time, user, attack, and location, and helps the administrator configure security policies in a refined manner.

Application Awareness

The application awareness module identifies unknown traffic and packet formats, extracts the signature, payload length, content or length change rule, IP address, and port of a packet, and incorporates statistics on and relationship of packets to accurately categorize applications of the traffic.

Huawei cloud security competence center, by virtue of its experience and expertise, provides an application signature database that covers more than 6000 applications. The USG6000 series can use the application identification engine and online update of the signature database to identify and track the latest applications.

- Application-specific security control

The USG6000 series implements application-specific security control to categorize traffic in a fine-granular manner and accurately control the traffic. For example, the USG6000 series permits HTTP traffic and denies traffic of WebThunder.

Based on unified policies, application-specific security policies has integrated the application dimension. The policy meaning and configuration mode remain unchanged.

- Application-specific traffic management and control

The USG6000 series implements application-specific traffic management and control to categorize traffic in a fine-granular manner and accurately control the traffic. For example, the USG6000 series limits the bandwidth of P2P applications to guarantee bandwidth for internal applications.

Based on bandwidth policies, application-specific security policies has integrated the application dimension. The policy meaning and configuration mode remain unchanged.

Traffic management and control of the USG6000 series support the guaranteed bandwidth and maximum bandwidth. The guaranteed bandwidth specifies the minimum bandwidth resources for key services to prevent other services from occupying too much bandwidth. The maximum bandwidth specifies the maximum bandwidth resources of some services to prevent the impact on other services.

- Application-specific PBR

The USG6000 series implements application-specific PBR to apply different route selection policies by application. For example, the USG6000 series selects a reliable and low-delay link for key information system applications of enterprises and other links for P2P applications.

Based on PBR policies, application-specific security policies has integrated the application dimension. The policy meaning and configuration mode remain unchanged.

Content Awareness

The USG6000 series analyzes application protocols to obtain the content transmitted by the application protocols and applies security policies by content.

The content awareness module consists of a protocol decoding module and a content matching module. The protocol decoding module categorizes incoming packets by protocol, obtains information based on the category, decompresses and unpacks the obtained files, identifies real file types, sorts the obtained URLs, and sends them to the content matching module. The content matching module matches traffic information with virus signatures, intrusion rule signatures, sensitive information, and email contents and determines whether the traffic triggers security policies based on the matching results. The signatures can be updated on the cloud, or traffic information can be sent to the cloud for detection, which ensures the up-to-date and effectiveness of signatures.

Time Awareness

The USG6000 series implements time awareness based on the following technologies:

- Automatic clock synchronization

The USG6000 series uses Network Time Protocol (NTP) to obtain standard network time and adjust the local clock.

- Automatic conversion of DST

Some countries and regions use the DST system. The USG6000 series sets the DST clock based on the VRP, and the device clock is automatically switched with the DST clock.

- Time-specific security policy

The USG6000 series has integrated the time or time segment into the security, traffic control, and authentication policies as a matching condition and updates the policies by time or time segment to implement time-specific control. You can configure the USG6000 series to apply traffic control policies on network traffic by time segment.

User Awareness

Enterprise networks become borderless with increasing mobile office employees whose IP addresses are dynamically changed. The security policies of traditional firewalls are based on IP configurations, which cannot meet requirements on security management and control. How to accurately identify users and effectively manage and control user behaviors has become a top issue of network security.

User awareness of the USG6000 series identifies users of network traffic and implements security management and control by user.

- User authentication and identification

  User identification is the prerequisite of applying differentiated policies on users. The user management and control module provides multiple authentication modes to meet the requirements of different user types and scenarios.

  - Authentication exemption

  Upper executives require high efficiency and authentication exemption. However, their activities must be highly secure. You can bind their accounts to IP or MAC addresses and configure authentication exemption for them. The USG6000 series then exempts upper executives from authentication and allows the login only from the bound IP or MAC address.

  Some enterprises have guests who may need to access the enterprise networks. The guests do not have dedicated accounts and cannot be authenticated. Therefore, their network access permissions must be controlled. To accommodate this situation, the user management and control module automatically creates temporary accounts for the guests with their IP addresses as user names.

  - Password authentication

  For common employees, password authentication is applied.

  Users can access the URL of an authentication page before starting service access. The USG6000 series supports HTTP and HTTPS authentication. You are advised to choose HTTPS authentication to meet high security requirements.

  The USG6000 series supports authentication based on user names and passwords. It can also interwork with the LDAP, RADIUS, and AD authentication servers and send user information to the authentication servers.

  In addition, the USG6000 series supports redirected web authentication. When an unauthenticated employee accesses HTTP services, the USG6000 series redirects the user to an authentication page and prompts the user to get authenticated.

  - Single Sign-On (SSO)

  If an AD server with an identity authentication system has been deployed on a network, the USG6000 series can interwork with the AD server to implement SSO. After identifying that a user is authenticated by the AD server, the USG6000 series permits the user without requesting the user name and password.

  If a user has used a VPN (such as an L2TP or SSL VPN) for access and the USG6000 series has authenticated the user, the USG6000 series normalizes the access user and the user whose online behaviors are managed to implement SSO and avoid re-authentication.

  - User-initiated authentication and redirected authentication

  User-initiated authentication is an authentication mode that a user logs in to the authentication portal page of the USG6000 series for authentication

before accessing network resources. User-initiated authentication supports all access methods.

Redirected authentication is an authentication mode that an unauthenticated user accesses network resources and the USG6000 series identifies that the user is not authenticated and pushes an authentication page to the user. Redirected authentication supports only HTTP access.

- User-specific management and control policy
  - Online user management and control

To restrict all online behaviors of some users within a time segment, you can lock out the online users.

You can also force some untrustworthy online users to log out.

- Policy management and control

The USG6000 series supports user-specific online behavior management that includes application-layer management and control functions, such as user-specific and quintuple-based behavior control, user-specific application-layer protocol control, user-specific URL access control, mail filtering, and file filtering by keyword or type. For example, you can forbid instant messaging tools such as Skype during working hours and forbid the access to certain game or forum URLs to ensure working efficiency.

The USG6000 series provides user-specific traffic management and control and limits the number of concurrent connections by user to effectively allocate and manage bandwidth resources. The USG6000 series can audit and analyze the traffic statistics of users and user groups for follow-up optimization.

The USG6000 series provides reports, such as user-specific traffic rankings by category and time

Users can inherit management and control policies from user groups, and the user groups can inherit the policies from parent user groups.

Attack Awareness

Attack awareness of the USG6000 series identifies network security events and content security events and incorporates the awareness results of attack events, attack behaviors, and abnormal traffic into the reports of unified security policies and security postures. Attack awareness enables the USG6000 series to defend against attack behaviors and provides administrators and CIOs visibility into security postures for accurate understanding.

Huawei security R&D team has sustained accumulation of attack awareness technologies as follows:

- DoS/DDoS detection and defense

The USG6000 series provides powerful DDoS detection capabilities based on the behavior analysis, legitimate traffic identification, feature identification and filtering, abnormal traffic baseline learning, dynamic fingerprint identification, reverse source detection technologies to detect malformed packet attacks (such as Winnuke and Teardrop), scanning and sniffing attacks (such as the IP sweep, port scanning, and IP source routing option attacks), and flood or traffic attacks. The USG6000 series also incorporates the Netstream and route-based traffic

injection and diversion technologies and interworks with the upstream and downstream devices to implement DDoS detection, layer-specific attack traffic cleaning, and attack defense on the entire network.

- IPS

Botnets, Trojan horses, worms, SQL injection attacks, and XSS attacks are predominant on the Internet. The USG6000 series has integrated IPS that provides the in-line deployment mode to proactively detect and block intrusion behaviors.

IPS of the USG6000 series uses Huawei-proprietary integrated detection engine and multi-core hardware platform with acceleration feature to obtain high-performance detection capabilities. The predefined and user-defined detection rules, online update of the engine and signature database, and intrusion tracking results of Huawei security attack defense lab enable the USG6000 series to accurately detect intrusions and zero-day attacks.

- AV

AV of the USG6000 series detects and blocks the files infected with viruses based on the flow reassembly, file reassembly, unpacking, decompression, PE virus detection, and flow-based heuristic detection technologies. The engine and virus database of AV also supports real-time online updates.

- Spam detection

Anti-spam of the USG6000 series detects spam and enables the data filtering and management and control of incoming and outgoing emails based on the Real-time Blackhole List (RBL) technology using dynamic blacklists and real-time filtering of emails over SMTP, POP3, and Webmail.

- Malicious URL detection

Malicious URL detection of the USG6000 series blocks access to malicious websites such as the Trojan horse and phishing websites. Huawei security team maintains malicious URL categories to be up to date. The malicious URL categories of the USG6000 series support real-time online query and update.

In addition, attack awareness of the USG6000 series has powerful cloud security capabilities. The USG6000 series collects and sends all attack awareness results to cloud servers for analysis and processing, obtains Internet security postures, and synchronizes real-time detection capabilities from other devices.

Location Awareness

Location awareness of the USG6000 series analyzes the location (such as the city, region, or country) that traffic is initiated from or destined for based on the source and destination IP addresses.

The USG6000 series incorporates the network address and geographical location information and integrates user-defined locations and location sets into unified policies to provide location-specific security policies, traffic limiting policies, routing policies, audit policies, and statistics and reports of traffic and threats.

The USG6000 series implements location awareness as follows:

- Location-specific policy configuration

Location-specific policy configuration helps you manage users and traffic by location. The USG6000 series can provide the security filtering, bandwidth control, authentication, and audit policies based on location awareness. For example, you can configure location-specific security policies to allow Internet users in Hong Kong and London to access intranet resources and prevent Internet users of the USA from accessing the resources.

- Location-specific traffic statistics collection, threat statistics collection, and analysis

The USG6000 series automatically collects location information of the local device and packets, analyzes traffic, threats, and security threats by location, and provides location-specific traffic and threat trend reports. The reports provide you visibility into traffic rankings by source location and destination location. You can click a location to view all statistics and trends of the location.

Unified Policy

The USG6000 series supports the configuration of security policies based on the quintuple as well as application, user, time, and location. The USG6000 series provides unified policies to integrate all policy conditions and a unified configuration page. The unified policy features the following aspects:

- Unified configuration page

You can configure all conditions such as the quintuple, application, user, time, and location in one policy rule. The USG6000 series provides a unified page for policy configuration and maintenance.

Each policy rule can be bound to application-layer profiles such as the IPS, AV, and Data Loss Prevention profiles.

- Unified processing flow

The USG6000 series provides a unified processing flow of policies. Different features at the same layer require only one resolution and policy matching process, which prevents the waste of system resources.

3.6 SmartPolicy

The NGFW has changed the quintuple-based policy configuration of traditional firewalls into refined policy configuration by user and application. The system administrator faces a variety of applications, categories, and protocols during policy management.

The NGFW provides threat detection functions such as IPS and AV and a large number of threat features and virus features. More and more security policies are configured in the system during the operating. Many low-efficiency, conflicting, and redundant policies exist. The system administrator must take a long time to configure and manage the policies.

In addition, the system administrator must understand application features to correctly use the defense and protection technologies, because application-layer security defense is complex. Therefore, firewall policy management brings about great challenges.

SmartPolicy intelligently analyzes network traffic, identifies common applications, and obtains the percentage of all application traffic. SmartPolicy generates a series of security defense policies according to possible threats of an application, which simplifies the configuration process.

SmartPolicy consists of the following actions:

- Traffic learning and analysis

The USG6000 series implements application analysis on traffic using the application awareness technology and provides the proportions of traffic generated by all applications and behavior models of application traffic. Based on the analysis result, the USG6000 series identifies possible threats and provides reference for follow-up policy pushing and optimization.

- Policy pushing

According to the traffic learning and analysis results, the USG6000 series identifies the proportions of application-specific traffic and behavior models, analyzes threats and risks, and generates recommended policies based on the traffic and risk status. These policies include integrated policies and application-layer security profiles, which help administrators in policy configuration.

- Policy optimization

The USG6000 series analyzes existing integrated policies and generates optimized policies. Static analysis and dynamic analysis are implemented as follows:

Static analysis: The USG6000 series analyzes the configurations of existing integrated policies in terms of conflict and redundancy and provides optimization references. It also analyzes policy validity based on the traffic learning and risk identification results and provides optimization references.

Dynamic analysis: The USG6000 series collects statistics on the matching status of all integrated security policies and displays the policy trend and distribution of policies that are seldom matched for administrators to reference.

3.7 Advanced Virtual Firewall Technology

Nowadays, large cross-region enterprises and organizations are blooming in business scale and management complexity, and traditional management modes cannot follow the business development any longer. Informationization, however, effectively breaks through the bottleneck and has become a hot concern. With the increase of business scales, the functionality and responsibility of each division are much clearer; and security zones with different priorities are also formed in each division, for example, the OA and data center. All these factors pose high security requirements on certain important security zones in an enterprise.

How to realize flexible and convenient security zone division and controllable communication among security zones becomes an urgent challenge for information administrators of enterprises.

To meet the previous requirements, a firewall is deployed in front of each service VPN to implement access control over department networks.

Obviously, the number of service VPNs in an enterprise increases sharply with the rapid business development. The traditional deployment cannot adapt to new application environments as follows:

- Many independent firewalls must be deployed and managed due to the large number of divisions, resulting in high TCO.
- The centralized deployment of independent firewalls occupies large subrack space and complicates the cabling.
- The VPN division varies with business development. As a result, physical change is required by traditional firewalls, bringing about difficulties in future component preparation and management.
- The deployment of additional physical firewalls increases network management complexity.

The virtual firewall technology emerges for this service mode. With the technology, a physical firewall is divided into multiple logical firewall instances to apply independent security policies for each service VPN. In addition, intranets can adjust to new services through flexibly deployed logical firewalls. When service classification changes or a new service department appears, the user can expand the network accordingly by adding or deleting firewall instances. In this manner, the deployment of network security devices is greatly simplified.

In addition, physical firewalls are replaced by virtual firewalls. This greatly reduces the number of devices to be managed and the complexity of network management and prevents possible misoperations.

Each virtual firewall can be independently configured with resources to avoid impacts from other virtual firewalls during the operating process. Resources available to virtual firewalls fall into two categories: configuration resources and operating resources. Configuration resources are the resources that can be configured by virtual firewall administrators, including the user group quantity, user quantity, and policy quantity. Operating resources are the service specifications when virtual firewalls are operating, including the session capacity, online user quantity, and bandwidth.

3.8 Service Support

Perfect Protection for Multi-Channel Protocols

The USG6000 series provides powerful service support capability. The major advantage of the USG6000 series is the implementation mode that combines connection status–based core technology and the dynamic and real-time policy modification. The USG6000 series can accurately identify dynamic ports

generated by service negotiations and dynamically adjust policies to guarantee security when ensuring the normal running of services.

The dynamic and real-time policy modification enables the USG6000 series to dynamically modify policies for multi-channel protocols. The dynamic policy works as a temporary entry. When packets of the data channel arrive, the USG6000 series matches them with the dynamic policies to determine channels that allow packets through. The USG6000 series then sets up a complete flow-based channel for the data channel and deletes the dynamic policies.

Data Flow Management for All Services

During data flow management, the USG6000 series dynamically identifies diversified services. For example, the USG6000 series can accurately identify FTP control flows, FTP data flows, Telnet data flows, and dynamically negotiated RTP and RTCP data flows. Because the negotiated data channels such as RTP, RTCP, and FTP data flows cannot be identified by ACLs, common routers and firewalls cannot implement control and QoS over these data flows.

Based on accurate identification of data flows, the USG6000 series implements differentiated control policies over data flows. For example, the USG6000 series allows longer idle time for Telnet data flows, but shorter for FTP data flows, or collects accurate statistics on the data flows of each service, such as the proportion of the passing data flows.

With accurate data flow identification, the USG6000 series presents great strengths in the optimization of networking resource allocation.

Comprehensive Service Capacity

The USG6000 series supports various complex services and is advantageous in networking environments with complex services.

It provides comprehensive support for each protocol to process network services. For example, H.323 is a complex protocol, and most firewalls cannot fully support H.323 applications. The USG6000 series, however, supports all networking models of H.323, including the MCU, GK, video terminal, and voice terminal.

Huawei has been engaged in data communications for many years and accumulated abundant technologies and experience. This is why the USG6000 series can provide such excellent service capabilities for diversified services.

Perfect Multi-Media Services

The USG6000 series supports various multi-media protocols, including H323, RAS, MGCP, SIP, and MMS. With these protocols, the USG6000 series not only ensures the security of multi-media service networks, but also isolates data services and voice services.

All service features of the USG6000 series support NAT that improves serviceability on intranets. Moreover, the USG6000 series provides the most comprehensive support for voice services. Most firewalls in the industry do not

fully support multi-media services and therefore cannot work with high performance on VoIP networks.

3.9 NAT

Excellent Performance

The USG6000 series uses connection-based address translation. It maintains a session entry for each connection and uses optimized algorithms during the processing to ensure outstanding address translation performance. Its performance deteriorates slightly with the enabling of NAT, so the NAT service provided by the USG6000 series will not become a network bottleneck.

Flexible Management

The USG6000 series provides the management function based on security zones. It logically divides the managed network by such factors as functional area and security requirement into multiple logical subnets according to the security zone concept. Each logical subnet is called a security zone. By default, the USG6000 series provides four security zones: Trust, Untrust, DMZ, and Local. The Trust zone connects to the intranet, the Untrust zone connects to the Internet, and the DMZ connects to internal servers such as the mail server and FTP server. The NAT function of the USG6000 series is configured for the access between different security zones, and therefore network management can be conveniently implemented. For example, if internal servers have sufficient public IP addresses, the public IP addresses can be directly used in the DMZ-Untrust interzone without any network translation. NAT is implemented in the Trust-Untrust interzone because the intranet uses private IP addresses.

The NAT function can interwork with ACLs that are used to control the range of address translation. Therefore, you can easily set address translation rules on the USG6000 series even if the public network and private network are mixed in the same zone.

Powerful Internal Servers

Internal servers enable Internet users to access resources on the intranet, such as web services. Many firewalls provide static mapping to enable such access. That is, a private address is bound to a public address. The biggest disadvantage of static mapping is that it consumes lots of legitimate IP addresses.

For example, the IP address of a host on the internal LAN is 10.110.0.0/24, and the LAN is connected to the Internet using a private line, with the public IP address 202.38.160.1 obtained from an ISP. If a web server at 10.110.0.1 is deployed on the LAN, you can configure static mapping to bind 10.110.0.1 to 202.38.160.1, so that Internet users can access the web server at 10.110.0.1 using 202.38.160.1. In this case, an internal server is deployed. Because the only public IP address on the LAN is used by the web server and no DNS or FTP server is available, hosts on the intranet cannot access the Internet and the LAN fails to provide any services for Internet users.

Static mapping has the following shortcomings:

1. Static mapping severely wastes public IP addresses, even if it resolves the reverse access issue. The NAT technology saves public IP addresses. However, public IP addresses cannot be fully used in static mapping mode.
2. Big security problems may occur. An internal server serves only a single purpose. For example, the web server provides only HTTP services. This server needs to provide access only to port 80. However, the web server deployed in static mapping mode enables Internet users to access port 80 and other ports, which bring about security risks. If a server can be maintained only at an intranet host using Telnet, static mapping may enable Internet hosts to telnet the server.
3. Servers with non-standard ports are difficult to deploy. For example, static mapping cannot be used to deploy two web servers, one using port 80 and the other using port 8080.

The NAT function of the USG6000 series supports port-level internal servers. You can configure internal servers in terms of ports and protocols for internal use and that for external use. In the previous example, if the NAT function of the USG6000 series is used, 202.38.160.1 can be used as the addresses of the web and FTP servers, and URL http://202.38.160.1:8080 can be used to deploy the second web server and users can use 202.38.160.1 to access the Internet.

The USG6000 series provides port-based mapping of internal servers. It can provide port-specific services and implement one-to-one mapping of addresses. Moreover, each USG6000 series provides the mapping of up to 4096 internal servers without affecting access efficiency.

Server Load Balancing

Server load balancing can be considered as a static address mapping extension. It provides the mapping of one public IP address and multiple private IP addresses. Traffic destined for the public IP address is balanced to servers at the private IP addresses on the server. Such a function improves server performance and reliability.

Server load balancing also provides port-level mapping to set up the mapping between a port of one public IP address and the ports of multiple private IP addresses. Based on the mapping relationship, the USG6000 series translates destination addresses and ports and forwards packets only when the packets are destined for the specified port of the public IP address.

Server load balancing implements heartbeat detection to check the server health. If a server becomes abnormal, subsequent requests are not forwarded to the server.

Perfect Service Support

NAT has difficulties in processing the packet whose payload contains address information. FTP packets are typical examples. The NAT function of the USG6000 series supports ICMP redirect, ICMP unreachable, FTP (in passive and active modes), H.323, NetMeeting, PPTP, L2TP, DNS, NetBIOS, SIP, MGCP, and Skype. Based on available services, the USG6000 series can

provide powerful service support to meet the requirements of most Internet services and prevent NAT from becoming a bottleneck in network services.

To better adapt to the development of network services, the USG6000 series provides a customized ALG function. The ALG of some service applications can be configured using command lines. Such a function strengthens the USG6000 series in its service support and response speed.

Furthermore, the architecture of the USG6000 series takes into account packet encryption and the rapid support for special protocols during address translation. Therefore, in terms of the application program gateway, the USG6000 series fully considers the program design and architecture. It can more quickly respond to user requirements and better support the ever changing network services.

Limitless PAT

The USG6000 series provides powerful PAT. PAT uses the port information of TCP or UDP and applies the "Address+Port" mode to identify connections initiated by hosts from the intranet to the Internet during NAT. In this manner, PAT enables users on the intranet to share one IP address to access the Internet.

The TCP or UDP port ranges from 1 to 65535. Ports 1 to 1024 are reserved by the system. Theoretically, a public IP address in PAT mode can support about 60,000 concurrent connections. The USG6000 series provides a Huawei-proprietary "unrestricted port" connection algorithm, which ensures that one public IP address can support infinite concurrent connections. This technology breaks through the upper limit of 65535 ports for Internet access in PAT mode, better meets requirements on address translation, and optimizes public IP addresses.

Multi-Interface Load Balancing

The NAT function of the USG6000 series supports Internet access using multiple interfaces in load balancing mode. In actual scenarios, intranet users may access the Internet using different interfaces or ISP networks. If address translation is not needed, you can configure two default routes on the USG6000 series to implement load balancing.

The address translation function of the USG6000 series supports the previous load balancing and Internet access using multiple interfaces. The function has an excellent effect in the Internet access scenario of a large intranet.

3.10 Diversified Attack Defense Methods

Excellent Necessary Capabilities for Defending Against DoS Attacks

DoS attacks are prevailing on the Internet. A DoS attack is to congest networks and interrupt services by sending various junk packets to the target. IP communication is connectionless. Attackers take advantage of this feature to invent various attack means. Launching a DoS attack is simple, even only a PC and a packet sending tool are used. Consequently, DoS attacks prevail on the

Internet and exert severe impacts on intranets and even backbone networks, leading to severe network accidents. Therefore, an excellent anti-DoS capability is indispensable to firewalls.

Almost all firewalls advertise anti-DoS functions. Why do DoS attacks frequently break down networks? An excellent anti-DoS system must have the following features:

- Provides comprehensive and diversified attack defense methods. The firewall must provide diversified methods to defend against DoS attacks, because they are launched using different means.
- Has excellent processing capabilities. An important feature of DoS attacks is the sudden increase of network traffic. If a firewall does not have excellent processing capabilities, the firewall itself becomes a bottleneck when processing the traffic of DoS attacks. Defending against the DoS attacks is impossible. A DoS attack is to make the target network paralyzed. If network congestion occurs on a key device, the attack objective is achieved. Note that you must consider forwarding performance and service processing capabilities of a firewall. In the anti-DoS defense process, the number of new connections per second is a key index to ensure network connectivity. Attackers randomly change source addresses to launch DoS attacks, and all connections are new ones.
- Has accurate attack identification capabilities. When processing traffic of DoS attacks, many firewalls only ensure that the traffic passing through them falls into an acceptable range, but cannot accurately identify attack packets. Such processing ensures the normal network traffic and server operating, but blocks legitimate users from accessing the Internet. The network plane is normal, but services of the legitimate users are denied. Therefore, the firewalls still fail to defend against DoS attacks.

The USG6000 series has thoroughly considered all the previous aspects, so it has big advantages over other firewalls in anti-DoS performance and functionality.

Diversified Anti-DoS Methods

The USG6000 series can defend against DoS attacks, such as ICMP flood, SYN flood, and UDP flood attacks based on the characteristics of data packets and the attack means. The USG6000 series proactively identifies dozens of common attack types. Many types of attacks may result in DoS. The USG6000 series can proactively detect and block illegal attacks to protect the intranet. The USG6000 series can be used to set up a secure defense system that has various attack defense methods to protect the network from DoS attacks.

The USG6000 series uses some unique defense technologies according to attack features to ensure that it can more specifically defend against DoS attacks and provide a complete attack defense feature.

In addition to careful consideration of attack means, the USG6000 series has fully taken into account the usage and network adaptability. The attack defense may protect a host or all hosts in a security zone.

Advanced TCP Proxy

The USG6000 series can use TCP proxy to prevent DoS attacks such as SYN flood, which may quickly exhaust all server resources and crash the server. The common anti-DoS technology cannot accurately identify traffic of legitimate users and attack packets when attacks are launched. The USG6000 series uses transparent TCP proxy to defend against DoS attacks. It can accurately identify attack packets based on precise authentication, allow the normal packets to access firewall resources, and discard attack packets directly.

Some attacks set up complete TCP connections to exhaust server resources. The USG6000 series implements an enhanced proxy function. It checks whether the client has any data packet to send after the connection with the client is established. If yes, the USG6000 series connects to the server. If no, the USG6000 series discards the packet from the client. Such a function ensures that the USG6000 series can identify the attacks that consume server resources even using the complete TCP three-way handshake.

Defense Against Scanning and Sniffing Attacks

Scanning and sniffing attacks use the ping sweep (ICMP and TCP) to identify the systems on the network, accurately locating potential targets. Alternatively, the scanning and sniffing attacks use the TCP and UCP port scanning to detect the potential services monitored by the operating system. Through scanning and sniffing, attackers can roughly learn about potential security vulnerabilities of and service types provided by the target system, preparing for further attacks.

The USG6000 series can flexibly and efficiently detect such scanning and sniffing packets using comparative analysis and prevent the subsequent attacks. Such scanning and sniffing attacks include address scanning, port scanning, IP Source Route attacks, IP Route Record attacks, and network structure sniffing through Tracert.

Malformed Packet Attack Prevention

The USG6000 series automatically detects attack packets and defends against the attacks that utilize malformed packets, including Land, Smurf, Fraggle, WinNuke, ICMP Redirect or Unreachable packets, illegitimate TCP packet flag bits (such as ACK, SYN, and FIN), Ping of Death, and Teardrop.

Defense Against Application-Layer DDoS Attacks

The anti-DDoS function of the USG6000 series defends against IP layer, transport layer, and application layer DDoS attacks such as the SIP flood, HTTP flood, HTTPS flood, DNS Request flood, and DNS Reply flood attacks. The USG6000 series automatically detects DDoS attacks. When a DDoS attack is found, the USG6000 series enables the anti-DDoS function to block attack traffic and permit normal traffic.

The anti-DDoS function of the USG6000 series supports threshold self-learning to provide references for the attack defense threshold setting and improve policy effectiveness. In normal cases, the system collects statistics on

various types of traffic by destination IP address and time, calculates the peak value of each traffic type, and automatically sets the defense thresholds.

3.11 High Networking Adaptability

High-Density Ports

The USG6300/USG6500 series includes the desktop model and the 1-U chassis model.

The desktop model of the USG6300/USG6500 series provides one console port and one USB port and supports eight fixed GE electrical interfaces. The desktop model provides an external power adapter.

The 1-U chassis model of the USG6300/USG6500 series provides one console port, one out-of-band management port (GE electrical interface), and one USB ports and supports eight fixed GE electrical interfaces and four fixed GE optical interfaces. The 1-U chassis model supports two SIC slots and one WSIC slot, two WSIC slots (two SIC slots can be combined into one WSIC slot), or one XSIC slot (two WSIC slots can be combined into one XSIC slot). The 1-U chassis model supports WSIC-8GE electrical interface card, WSIC-8GE optical interface card, WSIC-8GE electrical interface+2*10GE card, WSIC-2*10GE card, and WSIC-4GE electrical interface bypass card. In full configuration, the 1-U chassis model provides 16 GE electrical interfaces, four SFP optical interfaces, and four 10G optical interfaces. It supports dual power modules that are hot swappable and AC and DC power supplies.

The USG6600 series includes the 1-U chassis model and the 3-U chassis model

The USG6600 1-U model provides one console port or mini USB port (on the panel), one out-of-band management port (GE electrical interface), and two USB ports and supports eight fixed GE electrical interfaces and four fixed GE optical interfaces. The USG6600 1-U model supports two WSIC slots. The USG6600 1-U model supports WSIC-8GE electrical interface card, WSIC-8GE optical interface card, WSIC-8GE electrical interface+2*10GE card, WSIC-2*10GE card, and WSIC-4GE electrical interface bypass card. In full configuration, the USG6600 1-U model provides 24 GE electrical interfaces, four SFP optical interfaces, and four 10G optical interfaces. It supports dual power modules that are hot swappable and AC and DC power supplies.

The USG6600 3-U model provides one console port or mini USB port (on the panel), one out-of-band management port (GE electrical interface), and two USB ports and supports eight fixed GE electrical interfaces, four fixed GE optical interfaces, and two 10 GE optical interfaces. The USG6600 3-U model supports two WSIC slots and four XSIC slots or six WSIC slots. The USG6600 3-U model supports WSIC-8GE electrical interface card, WSIC-8GE optical interface card, WSIC-8GE electrical interface+2*10GE card, WSIC-2*10GE card, and WSIC-4GE electrical interface bypass card. In full configuration, the USG6600 3-U model provides 56 GE electrical interfaces, eight SFP optical interfaces, and fourteen 10G optical interfaces. It supports dual power modules that are hot swappable and AC and DC power supplies.

Diversified Routing Protocols and Routing Management

The USG6000 series provides abundant security features and has integrated some routing capabilities. The USG6000 series supports static routing, Routing Information Protocol (RIP), Open Shortest Path First (OSPF), routing policies, and route iteration. These functions make the networking of the USG6000 series more flexible. In addition, the USG6000 series supports Border Gateway Protocol (BGP) dynamic routing, which also improves networking flexibility.

Based on session flow–based PBR, the USG6000 series enables synergetic work between PBR and security features (such as NAT and ASPF) to implement load balancing on multiple egresses connected to ISP networks. When one link fails, the traffic fails over to other normal links.

Multiple Working Modes

The USG6000 series supports multiple working modes to enrich networking applications. The working modes are as follows:

Routing mode: The IP addresses of interfaces on the USG6000 series are fixed. Devices on the intranet and Internet has obtained the routes to the USG6000 series. You are advised to configure this mode for planning IP addresses in the initial phase of network construction to facilitate global network management.

Transparent mode: Interfaces on the USG6000 series are embedded between the intranet and the Internet, and no IP address is assigned to the interfaces. Devices on the intranet and Internet are unaware of the existence of the USG6000 series. This mode does not require the planning of IP addresses and routes and prevents the USG6000 series from intrusion.

Composite mode: The USG6000 series has both interfaces (with IP addresses) working in routing mode and interfaces (without IP addresses) working in transparent mode.

Diversified Authentication Methods

The USG6000 series provides a unified framework of authentication, authorization, and accounting and centralizes the security management of access to networks.

The USG6000 series provides local authentication and Remote Access Dial-In User Service (RADIUS) authentication. It also provides plain-text authentication and Message-Digest Algorithm 5 (MD5) authentication to support local user management. The USG6000 series can verify user identities, authorize legitimate users, and block illegitimate users.

The USG6000 series can interwork with Huawei-proprietary terminal security system to implement authentication when an internal host accesses the Internet or an intranet server. In this way, only the authenticated users can access the Internet or the intranet server. Meanwhile, the USG6000 series also checks whether a host is secure and whether operating system patches are installed. If the host is insecure, the USG6000 series isolates the host and prompts the user to repair it.

Multi-ISP Networking Adaptability

The USG6000 series delivers features such as PBR and multi-interface NAT to improve the multi-IPS networking solution. Users can configure PBR to specify two interfaces to share traffic. If one interface is faulty, all the traffic fails over to the other interface by the USG6000 series.

3.12 Excellent VPN Functions

The USG6000 series provides IPSec mechanisms based on software or hardware encryption (DES, 3DES, AH, and ESP) to offer services such as access control, connectionless integrity, data source authentication, anti-replay, encryption, and data flow classification and encryption to both parties of the communications. Through Authentication Header (AH) and Encapsulating Security Payload (ESP), data transmitted at the IP layer or upper layers are protected, and the tunnel encapsulation mode is supported.

In addition to supporting IPSec VPN application and providing highly reliable security transport channels, the USG6000 series can incorporate Layer 2 Tunneling Protocol (L2TP) and Generic Routing Encapsulation (GRE) to provide diversified VPN applications:

- L2TP VPN
- IPSec VPN
- GRE VPN
- SSL VPN
- L2TP over IPSec VPN
- GRE over IPSec VPN

GRE VPN

GRE, a Layer 3 tunneling protocol of VPNs, can add an IP header on the IP packet. In other words, GRE adds a "coat" on private data for secure transmission.

The USG6000 series not only supports the GRE VPN function, which sets up a GRE tunnel between two gateways to provide secure transmission, but also incorporates IPSec to provide diversified VPN applications.

L2TP VPN

The USG6000 series supports L2TP that implements the transparent transmission of PPP packets between users and enterprise servers, which is widely applied to access VPNs. Layer-2 data packets are encapsulated in a tunnel. For example, PPP packets are encapsulated in the L2TP tunnel.

When serving as an LNS, the USG6000 series allows mobile users to initiate L2TP tunnel connections and requires mobile users to install VPN Client and know the IP address of the LNS. After receiving the requests of mobile users, the USG6000 series authenticates the mobile users based on the user name and password, allocates private addresses for mobile users, and establishes tunnels.

The USG6000 series, serving as a LAC, initiates L2TP tunnel connections for users when they access the Internet. Users can access the Internet using PPP or PPPoE. When the user name and password are authenticated on the LAC, you can identify L2TP tunnel users by user name. The LAC automatically initiates connections to the LNS, and the user then can access the enterprise VPN.

Mobile users can use L2TP client software to connect to the LNS and access the headquarters intranet, but the IP address of the LNS, which is a private IP address, must be translated by the NAT server.

IPSec VPN

Using the IPSec mechanism, the USG6000 series provides security services such as access control, connectionless integrity, data source authentication, anti-replay, encryption, and data flow classification and encryption for communications parties. Data transmitted at the IP layer or upper layers is protected using AH and ESP, and the data can be encapsulated in tunnels.

IPSec provides the following types of network security services:

1. Privacy: Before transmitting packets, IPSec encrypts packets to ensure the data privacy.
2. Integrity: IPSec verifies packets at the destination to ensure that the packets are not modified during the transmission.
3. Authenticity: IPSec authenticates all the protected packets.
4. Anti-replay: IPSec prevents packet retransmission. That is, the earlier or the repeated packets are denied at the destination. The packets are denied by packet sequence number.

The USG6000 series uses the IPSec VPN to establish tunnels between the headquarters VPN gateway and branch VPN gateways and to obtain private addresses, securing the transmission and information. IPSec provides data protection between two hosts, two security gateways, or a host and a security gateway. Multiple security associations (SAs) can be established between two ends. By using ACLs and SAs, IPSec can apply different protection policies to data flows, to provide varied protection. IPSec SAs can be manually established. When the nodes on the network increase, it is difficult to configure SAs and ensure security. In this case, IKE is required to automatically establish SAs and implement key exchange. The IPSec VPN function of the USG6000 series provides the certificate authentication mechanism based on the PKI framework. This mechanism supports certificate application, storage, and authentication, but not certificate generation. In addition, this mechanism supports digital envelop-based IKE negotiation. That is, certificate authentication is used during IKE negotiation.

The USG6000 series supports IPSec VPN on IPv6, which provides VPN connectivity in IPv6 environment.

BGP/MPLS VPN

As a Layer 3 Virtual Private Network (L3VPN), BGP/MPLS IP VPN employs BGP to advertise VPN routes and MPLS to forward VPN packets on the backbone networks of ISPs. "IP" indicates that the VPN carries IP packets.

The Multiprotocol Label Switching (MPLS) technology combines the flexible IP routing and convenient asynchronous transfer mode (ATM) label switching. MPLS incorporates the connection-oriented control plane into the connectionless IP network to facilitate network management and operation.

Therefore, an MPLS VPN that uses the MPLS-based IP network as the backbone network has become an important method for IP network carriers to provide value-added services and attracts more carriers.

Unlike IGP, BGP focuses on controlling route advertisement and choosing the optimal route instead of finding and computing routes. VPN uses the public network to transmit data, where IGP route discovery and calculation have been applied. The primary concerns for constructing a VPN are controlling the spread of VPN routes and choosing the best route between two PEs.

BGP uses TCP (port 179) as the transport protocol to improve reliability. Two USG6000-connected PE devices can run the BGP protocol to exchange VPN routes.

BGP carries any information attached to routes as optional BGP attributes. The USG6000 series directly forwards the routes with any unknown attributes. Such processing facilitates the spread of VPN routes between PEs.

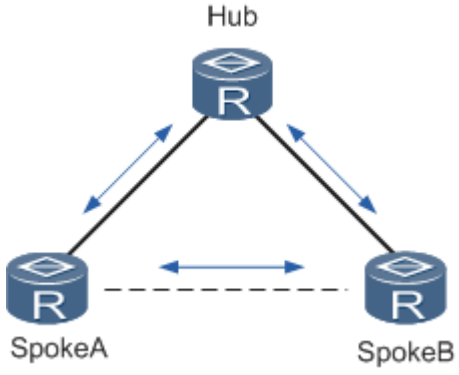
BGP sends only the updated routes, instead of all, to reduce the bandwidth for route transmission, making it possible to transmit a large number of VPN routes on the public network.

As an Exterior Gateway Protocol (EGP), BGP better applies to the VPN across carriers' networks.

DSVPN

Dynamic Smart VPN (DSVPN) is a technology that dynamically sets up a data forwarding tunnel between branches in the Hub-Spoke network model.

On a traditional Hub-Spoke network, data mainly flows between the Spokes and the Hub. If data exchange is required between the Spokes and the IPSec technology has been applied, the Hub decrypts data over the branch tunnel for receiving data and re-encrypts data over the branch tunnel for sending data. The data exchanged between Spokes passes through the Hub, consumes Hub resources, and brings about delays. The DSVPN technology enables dynamic establishment of a data forwarding tunnel between Spokes, which resolves the previous issue.



SSL VPN

Secure Sockets Layer (SSL) VPN is transparent to users and easy to manage, making it an attractive remote access security solution. An enterprise can expand its intranet anywhere on the Internet, including the PCs and Internet information platform, therefore promoting employee productivity, protecting enterprise data, as well as enabling partners and consultants to access the intranet.

Based on the SSL/TLS supported by all standard browsers, the SSL VPN has enhanced SSL/TLS functions.

SSL ensures data communication security in the following aspects:

- Authentication: Before the SSL connection is established, mutual authentication between the client and server is required, and the authentication uses the digital certificate. The authentication can be performed either by the client on the server or mutually on each other.
- Confidentiality: An encryption algorithm is used to encrypt the data to be transmitted.
- Integrity: A data authentication algorithm is used to verify the received data.

The proxy function of the USG6000 series helps you access web resources on the intranet using a web browser. Web proxy fully outstands the ease-of-use of SSL VPN. When a remote user sends a request to access intranet pages using a web browser, the USG6000 series receives and forwards the request to the intranet server, and sends the server response in web pages to the user. During transmission on the Internet, information of the web pages is encrypted in the SSL tunnel to ensure that web resources on the intranet are provided to remote users securely and truly.

3.13 Application-Layer Security

Service Awareness (SA)

Traditional firewalls identifies applications and applies policies by port. If an application uses an ephemeral port for communication, the application may evade the detection of firewalls.

SA of the USG6000 series implements in-depth analysis on packet payload to identify the real application type of traffic. It has the following features:

- Multiple identification methods

The USG6000 series uses several methods to accurately identify common protocols such as HTTP and applications such as facebook and WebMail.

- Predefined identification rule database

The USG6000 series incorporates a predefined rule database to identify applications. The rule database can be updated online to identify ever-increasing new applications.

Huawei predefined rule database supports more than 5000 protocols and applications to meet identification requirements.

- User-defined identification rules

The USG6000 series also supports user-defined rules for application identification to meet differentiated requirements.

You can define conditions such as the IP address, port, and content matching in application identification rules to identify protocols or applications that are not covered by the predefined rules.

Intrusion Prevention System (IPS)

IPS of the USG6000 series, based on in-depth application identification, implements application-layer analysis and detection on the traffic to accurately identify various network attack behaviors and defend against the attacks. The USG6000 series detects threats such as botnets, Trojan horses, and worms and attacks such as the SQL injection and XSS attacks.

- Deployment mode

Off-line deployment: The USG6000 series implements security detection, but not defense action or traffic cleaning. Traffic is free of any impact.

In-line detection deployment: The USG6000 series implements security detection, but not defense actions. It modifies only some QoS and TTL information but does not discard packets.

In-line defense deployment: The USG6000 series implements security detection and traffic cleaning. When a security threat is detected, the USG6000 series applies defense actions, such as discarding packets, modifying packets, and limiting traffic.

- Major features

Detection based on predefined rules: You can configure predefined rules for users, including the policies that defend against vulnerability-based attacks, botnets, Trojan horses, worms, SQL injection attacks, and XSS attacks. You can choose and generate a set of signatures by object, severity, operating system, protocol type, and threat type and formulate predefined rules based on the signatures. You can also define exception signatures to exempt some objects.

Detection based on user-defined rules: You can configure user-defined rules when necessary. A user-defined rule consists of the user-defined object and rule body. The rule body contains identification conditions for the decoded fields. Such a user-defined rule helps you flexibly meet the detection requirements for IPS.

Correlation detection: The USG6000 series provides predefined correlation detection for some threats to identify the relationship between security threat events. Such correlation detection helps you discover in-depth threats.

Anti-evasion: Hackers may evade the detection of IPS to attack the target device or server. Anti-evasion ensures accurate detection, without missing any attacks or threats.

Updates of the engine and signature database: The USG6000 series supports the online and offline updates of the engine and signature database to defend against new threats on the live network.

Antivirus (AV)

The AV feature of the USG6000 series implements application-layer inspection on traffic to analyze transmitted files, detect viruses, and blocks the transfer of virus-infected files, protecting the customer's server and PC.

The USG6000 series provides the following AV functions:

- Powerful application-layer protocol parsing

The USG6000 series implements powerful application-layer protocol parsing to analyze file transfer actions and scan files for viruses.

- Diversified file types

The USG6000 series supports diversified file types, decompresses file packages for virus scanning, and identifies the real file types based on content to prevent detection evasion that may be conspired by changing file name extensions.

- Flow-based AV detection

The USG6000 series supports flow-based AV detection for high defense performance.

- Update of the virus signature database

The virus signature database can be updated for the device to detect new viruses on the live network. AV detection will not be interrupted while the virus signature database is updated.

Data Filtering

Data filtering of the USG6000 series implements application-layer analysis on the transmitted data, detects and blocks data at the application layer based on predefined filtering policies, and reduces the risks of unauthorized file transfers and sensitive information transmission.

Data filtering consists of protocol data filtering, file blocking by type, and file blocking by data. They have different scanning and filtering objectives:

- Protocol data filtering

Some application-layer protocols carry information in protocol contents, such as the web page, forum, micro-blogging, and email contents. You can configure policies to filter protocol contents.

Based on in-depth protocol identification, the USG6000 series identifies traffic that uses an ephemeral port to prevent detection evasion and misjudgment.

The USG6000 series supports in-depth protocol decoding, multi-layer carrier protocol decoding, compression and decompression, and normalization to prevent application-layer detection evasion.

- File blocking by type

The USG6000 series filters application-layer files by type to block high-risk files and confidential files In addition, the USG6000 series filters transferred files by file name extension and real file type.

During the filtering by real file type, the USG6000 series identifies the real type of transferred files based on content to prevent detection evasion.

The USG6000 series decompresses compressed files and filters the files by real file type.

- File blocking by data

The USG6000 series implements in-depth analysis on file content and filters files by data to prevent information leaks and unauthorized information input.

During the filtering by real file type, the USG6000 series identifies the real type of transferred files based on content to prevent evasion.

The USG6000 series decompresses file packages and filters the files by real file type.

The USG6000 series also supports data normalization to prevent detection evasion using coding technologies.

HTTPS Traffic Defense

HTTPS traffic defense of the USG6000 series analyzes HTTPS traffic and provides application-layer protection after the decryption to prevent malicious traffic from evading detection through the HTTPS channel.

HTTPS traffic defense helps the USG6000 series decrypt HTTPS traffic. After the decryption is complete, the USG6000 series processes the traffic as it does to HTTP traffic. HTTPS traffic defense has the following operations:

- SSL proxy

SSL traffic cannot be decrypted in listening mode. To decrypt HTTPS traffic, the USG6000 series implements SSL proxy as follows:

1. After receiving an SSL negotiation request from a client, the USG6000 series serves as a server and negotiates with the client using its own certificate to set up an SSL tunnel.
2. The USG6000 series initiates SSL negotiation to the real server to set up an SSL tunnel.
3. The USG6000 series works as a transparent proxy server and forwards the traffic of the client and server. After receiving traffic from one tunnel end, the USG6000 series decrypts the traffic, implements application-layer detection, encrypts the traffic, and sends it to the other tunnel end.

- Application-layer detection

After SSL traffic is decrypted, the USG6000 series processes the HTTPS URL filtering as it does to HTTP traffic.

3.14 Sound Maintenance and Management System

Diversified Management Methods

The USG6000 series performs local or remote maintenance using the following methods:

- Local configuration and maintenance using the console port
- Local or remote configuration and maintenance using Telnet
- Secure Shell (SSH) maintenance and management. It provides information security guarantee and powerful authentication on an insecure network to defend against attacks such as IP spoofing and plain-text password interception.
- Web- and Webs-based GUI configuration and maintenance
- Unified management by Huawei NMS

SNMP-based Terminal System Management

The USG6000 series supports SNMP (v1/v2/v3) and the Client/Server model and can be managed by the NMS workstation such as Huawei eSight.

3.15 Comprehensive Log Report System

The USG6000 series collects statistics on the interface traffic and sessions during its operating to provide reference for the NMS, generate log information for other modules to make decisions, or deliver these information to users for debugging use. The users can customize logs by configuring the USG6000 series to collect statistics only on the interested information.

Logs are used to check the operating status of the device, analyze the network status, and locate the problem, providing references for system diagnosis and maintenance.

The system log of the USG6000 series provides an after-the-event audit mode. A router provides detailed logs on all operation records and attacks, as well as log query and filtering methods to facilitate log query and analysis.

The generated log information can be displayed using the console port or Telnet. It can be saved on a device or exported to the log server through the syslog protocol.

Local Log Storage

The USG6000 series supports hard disk cards to store generated logs.

When no log server is configured, you can use the local hard disk to store logs. If the local hard disk is full, you can enable the USG6000 series to discard the latest logs or use the latest logs to overwrite the oldest logs.

You can export log files from the hard disk to prevent log loss.

Log Server

To receive and store router logs, Huawei has launched dedicated log server software. Based on this software, users can conveniently browse, query, and analyze logs. The log server software consists of the front-end management and back-end process parts. Front-end management provides operations, such as database configuration, log configuration, and log category query. Back-end processes include the log collection and monitoring processes. You can use the log server software to customize receiving log types and provides log storage, query, export, and backup functions.

Two Log Export Modes

The USG6000 series supports the output of syslogs in text. In addition, the USG6000 series can create information tables based on flow status and generate fast binary logs for the heavy traffic passing through. Compared with syslogs, binary logs better suits the scenario in which log contents is massive and therefore require a higher network speed.

Abundant Logs

The USG6000 series provides complete and unified log information. The types of logs include:

- Traffic log

The USG6000 series generates traffic logs by flow for the passing traffic. A log of this type contains the source address, source port, destination address, destination port, Internet-access user, application, flow start time, flow end time, and flow status. For a flow that uses NAT, the related log also contains information about the address and port after NAT.

You can view global traffic conditions by user and application to learn about the bandwidth usage and security policy implementation.

- Attack defense log

When massive attacks occur, the USG6000 series applies the queue mechanism to provide log alarm information for the attack defense feature that routers support, and generates alarms in SYSLOG mode. Alarm information includes the attack source (source address) and attack type.

- Threat log

When detecting threats, the USG6000 series generates threat logs. The threat logs record the detected network threats such as viruses, intrusions, DDoS attacks, botnets, and worms and the defense against them. They help you learn about the current and historical threat events, modify policies, and take defense measures.

- URL filtering log

The USG6000 series implements URL filtering on intranet users who initiate web access based on the specified policy and records URL logs of the users. URL filtering logs help you learn about the URL access behaviors, alarms and blocking events generated when intranet users access URLs, and causes of the alarms and blocking events.

- Data filtering log

The USG6000 series implements data filtering and generates logs for the traffic that matches data filtering conditions. Data filtering logs help you learn about the risky user behaviors, alarms and blocking events generated when intranet users transfer files, send and receive emails, and access websites, and causes of the alarms and blocking events.

- Mail filtering log

The USG6000 series implements mail filtering and generates logs for the traffic that matches mail filtering conditions. Mail filtering logs help you learn about the protocol types, attachment quantities, and attachment sizes of user emails and the causes that legitimate emails are blocked and take appropriate measures.

- Operation log

Operation logs record all operations performed by administrators on the USG6000 series. The USG6000 series helps you learn about the logins, logouts, and configuration operations of all administrators and the device management history and enhance device security.

- System log

System logs record all key events during the system operating. Based on the logs, you can learn about the operating status of the device and locate the fault.

- User activity log

The USG6000 series logs user activities when the users access the Internet. User activity logs help you learn about user behaviors and user online records, such as the login time, Internet-access duration, and IP and MAC addresses used for login, discover abnormal user login and access behaviors, and take immediate measures.

- Policy matching log

The USG6000 series logs policy matching events. Policy matching logs help you learn about the events that policies are matched, determine whether policies are correctly configured and effective, and locate faults.

- Audit log

The USG6000 series supports the behavior audit and content audit functions and generates audit logs on user Internet-access behaviors and key contents. Based on audit logs, you can view the network behaviors of users.

- Traffic monitoring log

The USG6000 series monitors traffic by security zone and IP address, checks whether the rate or connection quantity reaches the upper limit or lower limit. The USG6000 series generates alarms and records logs when the upper limit is hit, and generates alarms to instruct the system to recover when the lower limit is hit.

- Blacklist log

The USG6000 series automatically adds the source IP address of any illegitimate user that it has detected to the blacklist and generates a blacklist log that records the host IP address and blacklisting reason.

- Statistics information

Flow statistics are recorded to help you learn about the operating status of a router. The flow statistics include total connection quantity, current connection quantity and half-open connection quantity, peak connection quantity, and discarded packet quantity.

Statistics on attack packet quantities help you learn about the status of attack events.

Diversified Reports

The USG6000 series provides diversified reports that combine log information and intuitively display the information. You can customize reports to obtain only the data of your concern.

Reports can be sent in an email to the administrator at the scheduled time.

- Traffic report

Traffic reports of the USG6000 series analyze traffic statistics, rankings, and trends by source address, destination address, user, application, application category, and application subcategory.

The USG6000 series summarizes data of traffic logs and generates intuitive reports in different dimensions, which provide you visibility into network traffic status and help you determine traffic management methods.

- Threat report

Threat reports of the USG6000 series analyze threat times trends and rankings by threat type, user, attacker, target, threat name, virus, and attack defense.

The USG6000 series summarizes data of threat logs and generates intuitive reports in different dimensions, which provide you visibility into latest threat behaviors, attackers, and victims and help you determine security defense methods.

- URL report

URL reports of the USG6000 series analyze URL access statistics, rankings, and trends by URL type and website.

The USG6000 series summarizes data of URL logs and generates intuitive reports in different dimensions, which provide you visibility into the URLs or websites that are access the most times and users who frequently access illegitimate URLs and help you determine URL filtering policies.

- Policy matching report

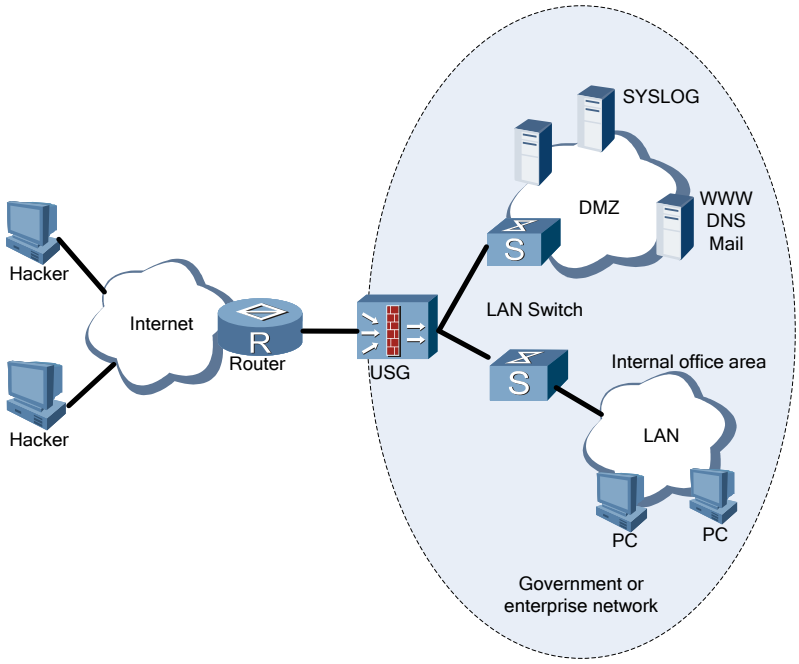
Policy matching reports of the USG6000 series analyze statistics on matching times and rankings by policy.

The USG6000 series summarizes data of policy matching logs and generates intuitive reports in different dimensions, which provide you visibility into policy configuration and effectiveness and help you optimize policies.

4 Typical Networking

4.1 Attack Defense

Figure 4-1 Attack defense networking diagram

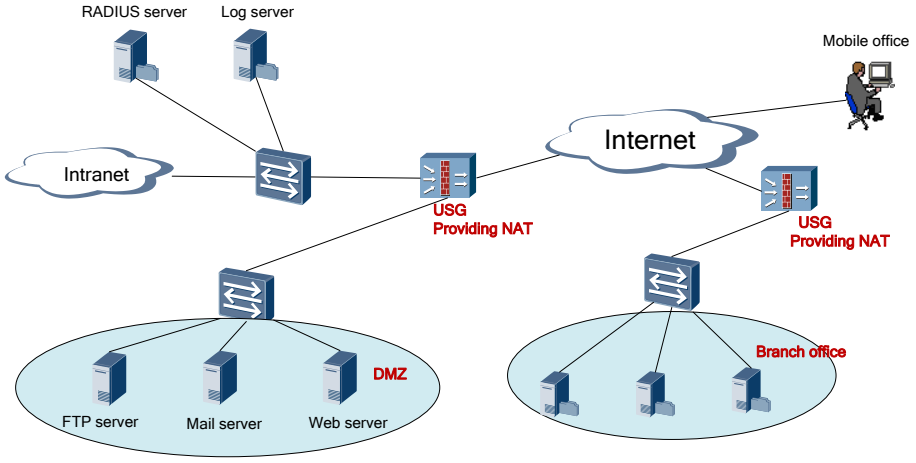


- The USG6000 series is deployed at the network ingress to prevent various attacks launched from the Internet and intranet.
- The available deployment mode is as follows: using the mirroring port of the device, LAN Switch, and unified security gateway to defend against various attacks.
- With the powerful anti-DoS function, the USG6000 series protects the resource hosts in the intranet to the greatest extent.
- The USG6000 series can work in transparent or routing mode to meet different networking requirements.

4.2 NAT

Combined with the policy-based NAT function, the USG6000 series establishes a more secure network environment using the secure filtering function over

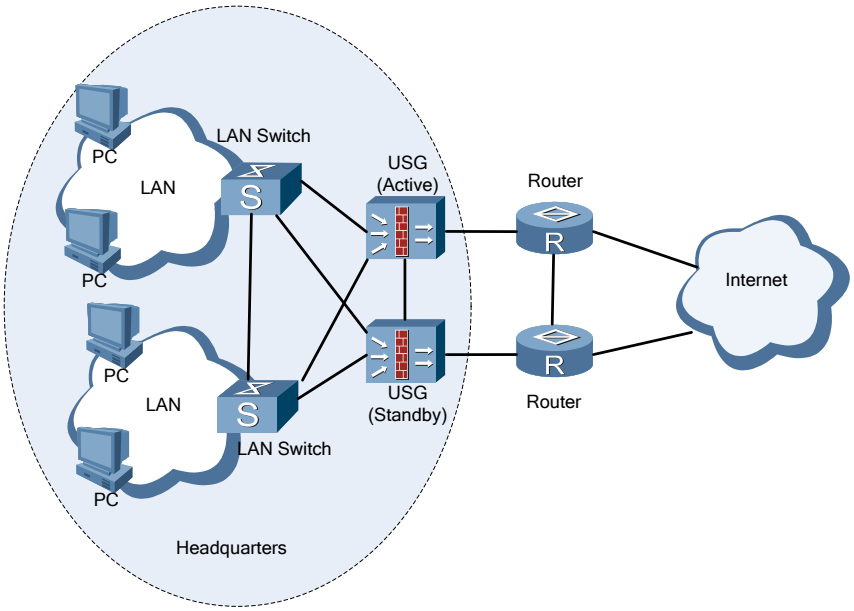
NAT applications to enhance capabilities in defending against attacks and preventing unauthorized access. The following figure shows NAT networking diagram of the USG6000 series.



- Specific users in the enterprise can access the Internet, e-commerce, and online banking systems, and a shield is set up between the intranet and the Internet.
- Remote branch offices or trustworthy partners can access internal servers (such as the web server and FTP server) in the DMZ through the firewall, but cannot access other intranet resources.
- Internet users cannot access resources on the intranet and the DMZ or launch any attacks.
- The USG6000 series supports bi-directional NAT and NAT ALG between the security zones of different security levels.
- The efficient logging function provides NAT logs.

4.3 Hot Standby

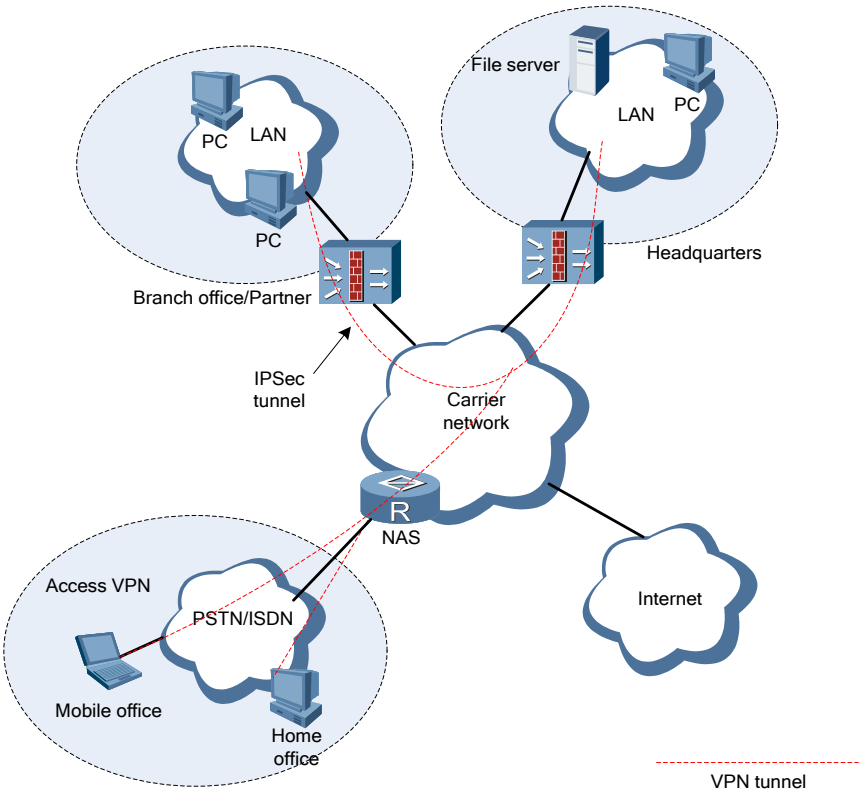
The USG6000 series supports hot standby, which ensures uninterrupted services even when the active and standby firewalls are switching over. The following figure shows the networking diagram for hot standby.



- Two USG6000s in the headquarters implement hot standby. One USG6000 functions as the active firewall and the other as the standby firewall to provide ACL, ASPF, traffic policing, NAT, and other security defense functions.
- The USG6000s are connected by the heartbeat link.
- The USG6000s are connected to intranet users through LAN switches.
- The USG6000s are connected to the Internet through routers.

4.4 VPN Applications Protected by IPSec

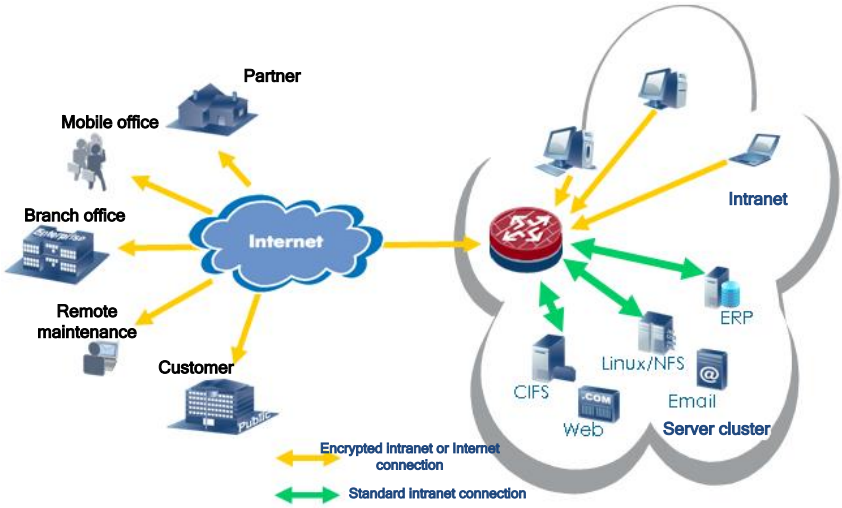
As VPN gateways, the USG6000 series supports the tunneling technologies such as L2TP and GRE. The IPSec, unified security gateway, and QoS technologies ensure the high quality and security of network information transmission. The following figure shows the networking diagram for the security VPN application.



- The Access VPN sets up a secure path for the SOHO and mobile office users to access the headquarters resources through PSTN/ISDN networks.
- Intranet VPN enables branch offices and representative offices to access resources at the headquarters. The IPSec and IKE technologies ensures the secure transmission of data on the Internet to prevent interception and tampering.
- The extranet VPN enables partners and customers to access the intranet and ensures the security of their own networks.

4.5 SSL VPN Application

Figure 4-2 SSL VPN solution



- Comprehensive user identity authentication, access authorization, and behavior audit to ensure legitimate user identities and implement refined access control policies
- Forcible encryption for the data between remote users and the intranet to protect sensitive data and prevent information leaks
- Support of a wide range of remote access services, including access to web resources, file systems, multiple types of C/S applications, and all-IP layer services that are irrelevant to applications
- Access through standard browsers, which means no need to install, configure, or maintain clients for users and effectively improves the productivity of mobile office personnel, such as employees on the move
- Excellent log functions, which facilitate the real-time audit and management of operation behaviors of administrators and other users

