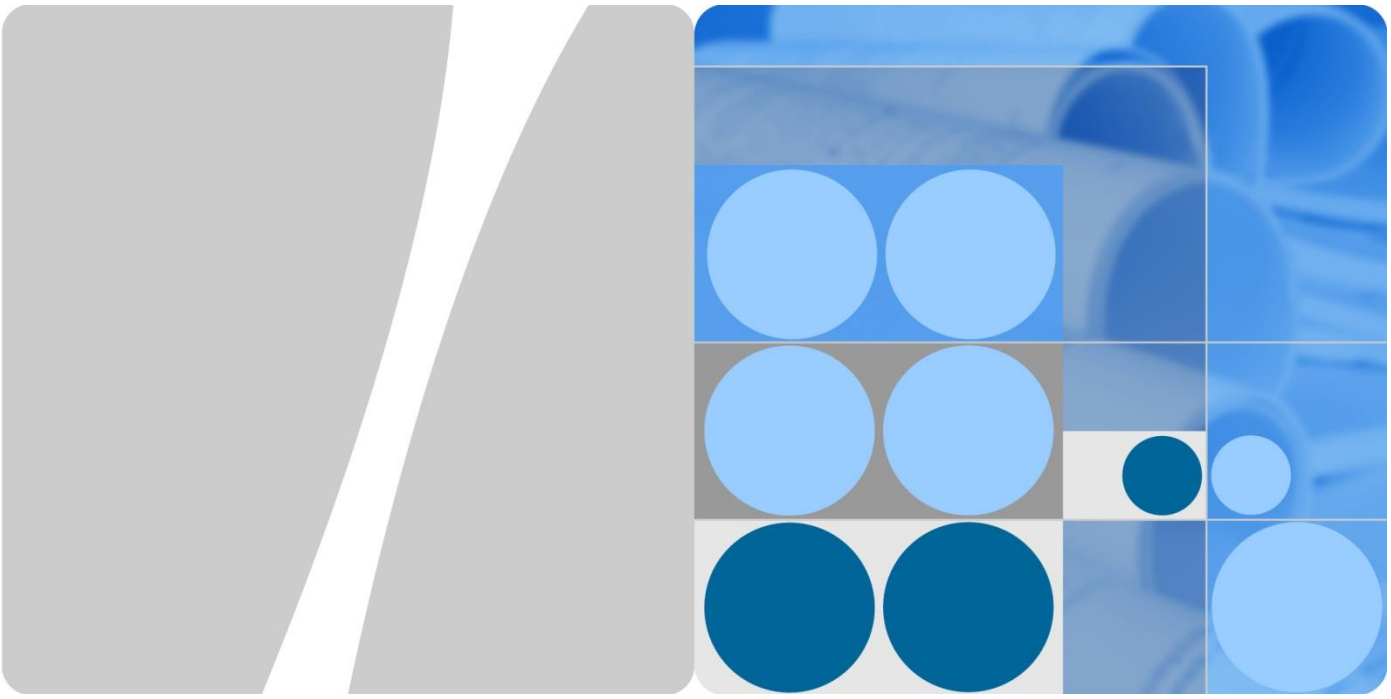


HUAWEI Secospace USG6000 Series Next-Generation Firewall

Feature Description

Issue V1.1

Date 2014-03-14

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: http://www.huawei.com

Email: support@huawei.com

Contents

1 Working Mode

1.1 Layer 2 Mode

Availability

This feature has been introduced since V100R001.

Summary

Service interfaces work at Layer 2 (the data-link layer). All the service interfaces belong to the same subnet and forward Layer-2 packets.

Benefits

The USG can be deployed as a Layer-2 bridge transparently in the existing network to implement Layer-2 switching and security defense without changing the existing network topology. The Layer 2 mode advantage is to control traffic in one subnet based on the MAC address without changing the existing network topology and configurations of adjacent devices.

Description

In Layer-2 mode, the USG is deployed as a switch that connects to the existing gateway without changing the network topology and configurations. Therefore, this deployment is also called the transparent mode. Layer-2 mode supports the following functions:

- Forwarding based on the MAC address

  In Layer-2 mode, the USG forwards packets based on the destination MAC address.

  After Layter-2 interfaces of the USG receive packets, the USG establishes a mapping relationship table of source MAC addresses and inbound interfaces. When forwarding packets, the USG searches the MAC address in the relationship based on the destination MAC address and forwards the packets to the mapped interface. If the MAC address has no mapped interface, the USG broadcasts to Layer-2 interfaces.

- VLAN isolation

  The Layer-2 mode can specify allowed VLANs. Then packets can be forwarded within the specified VLANs for security.

  The USG support Layer-2 access and trunk ports.

The USG implements routing and NAT if the service interfaces work at Layer 3, and implements transparent transmission if the service interfaces work at Layer 2.

Enhancement

The USG can be configured with both Layer-3 interfaces to implement Layer-3 gateway functions and Layer-2 interfaces to implement Layer-2 bridging functions.

Dependency

None.

1.2 Layer 3 Mode

Availability

This feature has been introduced since V100R001.

Summary

The service interfaces work at Layer 3 (the network layer). IP addresses of all Layer-3 interfaces cannot be in one subnet. Each Layer-3 interface connects to a separate subnet, and the USG forwards packets between subnets by IP address.

Benefits

In Layer-3 mode, the USG works as a router and can be connected to users' intranet and the Internet as a gateway without deploying a dedicated gateway.

Description

In Layer-3 mode, the USG can be deployed on a network as a router. Packets are forwarded based on the routing function. Therefore, this deployment is called the routing mode.

When deployed as a Layer-3 gateway between the intranet and the Internet, the USG also needs to translate between private addresses on the intranet and public addresses on the Internet. Therefore, this deployment is also called the NAT mode.

The IP address of each service interface is used as the default gateway address for all the PCs on the subnet. Therefore, when deploying a USG as a Layer-3 gateway, you may need to change the original network topology, routing data, and gateway configurations on PCs. When deploying a USG to replace the existing gateway, you are advised to use the original gateway configurations related to network layer protocols, such as IP addresses, routing protocols, and DHCP to avoid the change of configurations of adjacent devices.

- Forwarding packets based on the routing function

  IP addresses of all Layer-3 interfaces cannot be in one network segment. Each Layer-3 interface connects to a separate subnet. After the USG receives packets, it searches the routing table based on the destination IP address and forwards packets.

  The USG supports the static routing, dynamic routing (RIP, OSPF, and BGP), and policy routing.

The USG implements routing and NAT if the service interfaces work at Layer 3, and implements transparent transmission if the service interfaces work at Layer 2.

Enhancement

The USG can be configured with both Layer-3 interfaces to implement Layer-3 gateway functions and Layer-2 interfaces to implement Layer-2 bridging functions.

Dependency

None.

2 Web UI

2.1 Web UI

Availability

This feature has been introduced since V100R001.

Summary

The USG provides a web UI to manage common functions. An administrator can use a browser to configure and manage the USG through HTTP and HTTPS.

Benefits

- Enhances usability.

  A user can use a graphic UI to configure and manage the USG without running complicated commands, which enhances usability.

Description

The USG provides a web UI for visualized management and maintenance. The web UI supports HTTP, HTTPS, and the following functions:

- Wizard

  An administrator can follow the wizard to complete important configurations quickly. The wizard provides configuration order of multiple functions. Therefore, a beginner can complete device deployment quickly. The USG supports the following wizards:

1. Startup wizard

   The startup wizard guides a beginner to initiate the device quickly and to access the Internet.

   The quick wizard covers configurations of device name, administrator password, system time, Internet access parameters, and LAN parameters. The startup wizards can connect the intranet and Internet in most scenarios and enables the intranet host and device to access the Internet.

2. Feature configuration wizard

   The USG provides wizards for features with advanced configurations for quick deployment in multiple scenarios. IPSec configuration wizard is used as an example.

- Function configuration UI

  The wizard provides a graphic UI to configure common functions.

- Log and report

  The USG web UI provides diversified graphic logs and reports.

  On the UI, the administrator can find the reason of discarding packets, locate and troubleshoot faults, identify occurred security events, and analyze bandwidth usage. Based on these information, the administrator can understand the network status and adjust device configurations.

- Visualized diagnosis

  If a network or device is faulty, the administrator can use the visualized diagnosis function to locate faults quickly. The visualized diagnosis function features multiple diagnosis items for one fault. This function helps the administrator locate all possible causes at one time and provide diagnosis results and repair suggestions automatically.

Enhancement

Dependency

None.

3 Link Aggregation

3.1 Eth-trunk

Availability

This feature has been introduced since V100R001.

Summary

Eth-trunk is a method for link aggregation and binds multiple physical interfaces in parallel as a logical interface to increase bandwidth. These physical interfaces share one IP address and work as one IP link.

Benefits

- Increases bandwidth.

  Before link aggregation, a network connecting 100M interfaces must change ports, such as use a 1000M interface, for higher data transmission rate. This solution is expensive and does not apply to small- and medium-sized enterprises. Link aggregation can bind multiple interfaces and increase bandwidth at a much lower costs.
- Improves availability.

  An aggregated link can have multiple member interfaces and provide redundancy in case one of the links fails.

Description

The link aggregation binds multiple physical interfaces into a logical interface (Eth-trunk interface), which improves the link bandwidth. Each bound physical interface is called a member interface.

The link aggregation has active and inactive interfaces. The interface that forwards data is an active interface and the one not is an inactive interface. If an active interface is faulty, the inactive interface can become an active interface for service availability.

The link aggregation has the following two types based on Link Aggregation Control Protocol (LACP):

- Manual link aggregation

  Manual link aggregation is a basic method. In this mode, the administrator establishes Eth-trunk interfaces, adds member interfaces, and selects active interfaces without using the LACP.

- Static LACP

  In this mode, the administrator establishes Eth-trunk interfaces and adds member interfaces. LACP selects active interfaces.

Enhancement

Dependency

None.

4 User Authentication

4.1 Local Authentication

Availability

This feature has been introduced since V100R001.

Summary

In local authentication mode, user names and passwords are saved on the USG. An authentication is implemented on the USG.

Benefits

The USG can work as an authentication server without deploying a dedicated authentication serve. User names and passwords can be authenticated on the USG.

Description

In local authentication, user names and passwords are saved on the USG, and users can be authenticated on the USG. The USG local authentication can authenticate administrators and online users.

- Administrator authentication

  A USG administrator is a user that connects to the USG UI (CLI or web) and configures and maintains the USG.

  USG administrators are hierarchical with multiple administrative permissions.

  An administrator accesses the USG authentication UI (CLI or web) and enters the user name and password. The USG abstract the administrator information from the local database for authentication.

- Online user

  An online user in an enterprise needs to access the intranet and Internet through the USG. The USG manages online user in levels and groups, controls permissions based on user groups and user names, and limits accessible resources.

  The online user authentication includes user-initiated authentication or redirected authentication.

  In user-initiated authentication, a user logs in to the USG authentication portal page before accessing network resources. The user-initiated authentication supports all network accessing methods.

In redirected authentication, if a user accesses network resources, the USG judges whether the user is authenticated. If the user is unauthenticated, the USG pushes the authentication page to prompt users. The user-initiated authentication supports HTTP.

Enhancement

None.

Dependency

None.

4.2 Remote Authentication

Availability

This feature has been introduced since V100R001.

Summary

In remote authentication, user names and passwords are saved on the remote authentication server. The authentication is implemented on the remote server.

Benefits

- Requires no change of the authentication method.

  If a network has an authentication server, the USG can interwork with the authentication server and provide remote authentication without changing the authentication method.

Description

User names and passwords to be authenticated are saved on the remote authentication server. The USG and remote authentication server interwork to perform user authentication. The USG remote authentication can authenticate administrators and online users.

- Administrator authentication

  A USG administrator is a user that connects to the USG UI (CLI or web) and configures and maintains the USG.

  USG administrators are hierarchical with multiple administrative permissions.

  An administrator accesses the USG authentication UI (CLI or web) and enters the user name and password. The USG obtains the authentication information and sends the information to the remote authentication server. The remote authentication server performs authentication and sends the authentication result back to the USG.

  Administrator remote authentication supports RADIUS.

- Online user

  An online user in an enterprise needs to access the intranet and Internet through the USG. The USG manages online user in levels and groups, controls permissions based on user groups and user names, and limits accessible resources.

  Online user authentication includes portal page authentication methods using the USG and authentication server.

In the portal page authentication using the USG, an administrator accesses the USG portal page and enters the user name and password. The USG obtains the authentication information and sends the information to the remote authentication server. The remote authentication server performs authentication and sends the authentication result back to the USG.

In the portal page authentication using the authentication server, an administrator accesses the portal page of the authentication server and enters the user name and password. The authentication server obtains the authentication information, performs authentication, and pushes the authentication result to the USG

The online user authentication includes user-initiated authentication or redirected authentication based on the authentication time.

In user-initiated authentication, a user logs in to the authentication portal page of the USG or authentication server before accessing network resources. The user-initiated authentication supports all network accessing methods.

In redirected authentication, if a user accesses network resources, the USG judges whether the user is authenticated. If the user is unauthenticated, the USG redirects the user to the portal authentication page and prompts the user for authentication. The user-initiated authentication supports HTTP.

Online user remote authentication supports RADIUS, LDAP, AD domain, SecurID, TSM, and HWTACACS.

Enhancement

None.

Dependency

None.

4.3 Online User Monitoring

Availability

This feature has been introduced since V100R001.

Summary

With online user monitoring, an administrator can view online users, forcibly log out a specified user, and lock out or unlock online users.

Benefits

The online user monitoring function monitors behaviors of online users. An administrator can forcibly log out a specified user and lock out or unlock online users.

Description

After user authentication is complete, the USG saves an online user form, recording online user information and monitoring online users. The USG online user monitoring function can perform the following functions:

- View online users

  An administrator can view the following information of all authenticated online users:
- Login name (display name): a unique ID for a user
- Parent group: a user group that the user belongs to
- IP address: the IP address that a user uses for login
- Authentication method: local authentication, third-party authentication, and authentication exemption
- Login methods: Local, L2TP, SSL VPN, and IPSec
- Login time or lockout duration: If a user is locked out, the star time of locking out is displayed.
- Online duration or remaining lockout duration: If a user is locked out, the remaining lockout duration is displayed.
- Traffic (KB): traffic volume of an online user The USG can rank the traffic.

  When viewing online users, you can set search conditions by user group, user name, and IP address to view specified online users.
- Forcibly log out an online user

  An administrator can forcibly log out the specified online user. After the user is logged out, the user information is deleted, and the user becomes unauthenticated. After an online user is forcibly logged out, the user must initiate an authentication request again before being able to access network resources.

  If an online user has multiple IP addresses and you have forcibly logged out the online user at an IP address, the online user can still log in to the system using another IP address.
- Forcibly log out all online users

  After all online users are forcibly logged out, the users must initiate authentication requests again before being able to access network resources.
- Lock out an online user

  An administrator can lock out an online user, cancel the user's permissions on network resources temporarily, and specify the locking out duration.

  After an online user is locked, the user cannot access network resources, log out, or initiate another authentication request. After the lockout duration expires or the administrator unlocks the user, if the timeout period has not expired, the online user can once again access network resources. If the timeout period has expired, the online user needs to be authenticated again before being able to access network resources.
- Unlock an online user

  If a user is unlocked, the user can log in to the USG again and access network resources within permissions.

Enhancement

None.

Dependency

None.

5 NAT

5.1 Static Address Mapping

Availability

This feature has been introduced since V100R001.

Summary

Static address mapping translates public addresses into private ones and provides static mapping between public IP addresses and private ones.

Benefits

- Hides a server.

  Static address mapping creates the mapping between the private and public IP addresses of servers. If an external user access the public IP address of the server, the USG translates the public IP address into a private one based on the mapping and forwards packets to the private server. The USG replaces the source private address in the packets sent from the server and with a public address hides the server address.

Description

Static address mapping translates public addresses into private ones and provides static mapping between public IP addresses and private ones. This mapping is used to translate the IP address of the intranet server to a public address. Therefore, static mapping is also called NAT Server.

Static address mapping also provides port mapping by creating the mapping between the specified port for private IP addresses and the specified port for public IP addresses. Only when an external user accesses the specified port for a public IP address, the USG translates the destination address and port and forwards packets.

Enhancement

None.

Dependency

None.

5.2 Server Load-Balancing

Availability

This feature has been introduced since V100R001.

Summary

Server load balancing is an extended function of the static address mapping and provides mapping between one public IP address and multiple private IP addresses. Multiple servers with these private addresses share the traffic destined to the Internet based on load balancing policies.

Benefits

- Increases server bandwidth.

  The USG balances traffic load among multiple internal servers, which is similar to internal server cluster. You can increase the server bandwidth by adding internal servers.
- Improves server availability.

  The USG balances traffic load among multiple internal servers. If a server is faulty, other servers share the traffic, which improves the availability.

Description

Server load balancing provides mapping between one public IP address and multiple private IP addresses. Multiple servers with these private addresses share the traffic destined to the Internet based on load balancing policies, which improves the overall server performance and availability.

Server load balancing also provides port mapping by creating the mapping between the specified port for multiple private IP addresses and the specified port for one public IP address. Only when an external user accesses the specified port for a public IP address, the USG translates the destination address and port and forwards packets.

The USG balances load among servers using algorithms, such as polling, weighted polling, and hash.

The USG performs heartbeat detection on servers. If a server is abnormal, the USG does not send requests to the server any more.

Enhancement

None.

Dependency

None.

5.3 Dynamic NAT

Availability

This feature has been introduced since V100R001.

Summary

If an intranet user accesses Internet resources, dynamic NAT translates the source private IP address in packets to a public IP address. The mapping is not fixed. Only when an intranet user accesses the Internet, the USG performs dynamic NAT. A private IP address may be translated in to multiple public IP addresses.

Benefits

- Saves public IP addresses.

  Multiple private IP addresses can be mapped to a few public IP addresses based on a policy, helping intranet users share public IP addresses and access the Internet.
- Hides the intranet server.

  Only public IP addresses can be viewed without displaying users' private IP addresses. Address mapping takes effect only when a user initiates the Internet access. An Internet user cannot initiate the access of a private IP address.

Description

If an intranet user accesses Internet resources, dynamic NAT translates the source private IP address in packets to a public IP address. The mapping is not fixed. Only when an intranet user accesses the Internet, the USG performs dynamic NAT. A private IP address may be translated in to multiple public IP addresses.

- Port translation

  Dynamic NAT includes NAT-PAT and NAT-NOPAT based on port address translation.
- Public address selection

  The USG specifies public addresses in two ways. The first way is the address pool. The USG can configure multiple public addresses in an address pool and select one public address for mapping. The second way is easy-IP. The USG translates the source IP addresses to the IP address of an outbound interface.

The USG users symmetric NAT. The same triplet (protocol, IP address, and port) may be mapped to multiple external triplets (protocol, IP address, and port) in different access scenarios.

Enhancement

None.

Dependency

None.

5.4 ALG

Availability

This feature has been introduced since V100R001.

Summary

The USG provides NAT application level gateway (ALG) to resolve packet payload and identify and translate the key information in the payload. NAT ALG ensures that addresses are properly translated for multi-channel protocols, such as FTP, without losing functionality.

Benefits

The USG provides NAT application level gateway (ALG) to resolve packet payload and identify the channel negotiation information. NAT ALG translates a private IP address or port into a public IP address or port based on the NAT policy for multi-channel protocols.

Description

NAT changes only the address information in IP headers and the port information in TCP/UDP headers, but cannot change the address and port information in packet payload. However, for some special protocols, such as FTP, the packet payload also carries address or port information, and the address or port information in the packet payload is usually dynamically negotiated by the communication parties. Therefore, administrators cannot configure NAT rules in advance for the information. If the NAT device cannot identify and translate the information, these protocols cannot be properly used.

The USG provides NAT ALG to resolve packet payload and identify and translate the key information in the payload. NAT ALG ensures that addresses are properly translated for multi-channel protocols, such as FTP, without losing functionality.

Enhancement

None.

Dependency

None.

6 VPN

6.1 IPSec4

Availability

This feature has been introduced since V100R001.

Summary

Benefits

Description

Enhancement

None.

Dependency

None.

6.2 IPSec6

Availability

This feature has been introduced since V100R001.

Summary

Benefits

Description

Enhancement

None.

Dependency

None.

6.3 L2TP

Availability

This feature has been introduced since V100R001.

Summary

The Layer 2 Tunneling Protocol (L2TP) extends the Point-to-Point Protocol (PPP) model. L2TP allows a user who wants to access an intranet server to initiate a PPP connection to an L2TP access concentrator (LAC) or L2TP network server (LNS). The LAC or LNS authenticates the user. If the user is authenticated, the LNS allocates a private network address for the user to access the intranet server.

Benefits

The virtual private network (VPN) provides access service for enterprises, small ISPs, and mobile workers.

Description

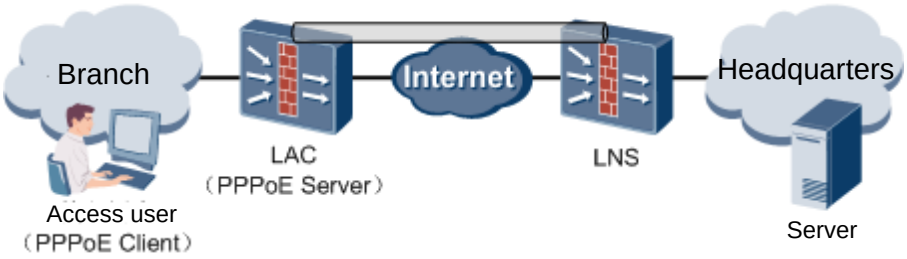
PPP defines an encapsulation mechanism for transporting multi-protocol packets across Layer-2 point-to-point links. For example, a user has a Layer-2 connection to a network access server (NAS) using the asymmetric digital subscriber line (ADSL) and then runs PPP over the connection. PPP allows a Layer-2 termination point and a PPP session endpoint to reside on the same physical device, such as a NAS. PPP connects users to the Internet, but cannot connect the users to the intranet at a branch office.

L2TP extends PPP to enable users to securely access an intranet. L2TP tunnels individual PPP frames to the NAS and extends the PPP model by allowing the Layer-2 termination point and PPP session endpoint to reside on different devices. With L2TP, a user initiates a Layer-2 connection to the LAC (NAS device) through PPP, and the LAC tunnels individual PPP frames to the LNS. Then a PPP connection is established between the user and the LNS. The Layer-2 termination point is the LAC, and the PPP session endpoint is the LNS. L2TP establishes a cross-LAC PPP link between the user and the LNS, and L2TP encapsulation is imperceptible to the user. L2TP allows both the LAC and LNS to implement user authentication to improve access security.

- L2TP roles

Figure 6-1 The basic networking diagram for the NAS-initiated VPN tunnel is shown in the following figure.

Figure 6-2 Basic networking diagram for the NAS-initiated VPN tunnel



The L2TP network consists of the following roles:

- User (also called an access user, client, or dial-up user)

  A user uses a host or routing device to connect to a private network. The user initiates a PPP negotiation and serves as an endpoint of a Layer-2 PPP link and a PPP session.

  The user can connect to the LAC from a private network or directly access the Internet to connect to the server at the headquarters.

- LAC

  A LAC, attached to a packet-switched network, is a device that has a PPP end system and L2TP processing capabilities to provide access for PPP users.

  The LAC resides and forwards packets between an LNS and a user. The LAC encrypts the packets from the user into L2TP packets and sends them to the LNS. Meanwhile, the LAC decrypts the packets from the LNS and sends them to the user.

  The connection from the LAC to the user is a local or PPP link. A PPP link is used in Virtual Private Dialup Network (VPDN).

- LNS

  An LNS, usually a device at the border of an intranet, serves as the PPP end system and L2TP server.

  The LNS is an L2TP tunnel endpoint, a peer to the LAC, and a logical termination point of a PPP session that is being tunneled by the LAC. With an L2TP tunnel, the remote end of the PPP connection is logically extended from the LAC to the LNS on the intranet.

- L2TP features

  L2TP has the following features:

- Flexible identity authentication and high security

  PPP implements PAP or CHAP authentication for L2TP to protect connections. L2TP has all security features of PPP.

  You can use tunneling encryption, end-to-end data encryption, or application-layer data encryption technologies together with L2TP to improve data security. For example, IPSec encrypts tunnel data.

- Multi-protocol transmission

  L2TP transmits PPP packets, and PPP transmits the packets of multiple protocols. L2TP encapsulates the packets of multiple protocols within PPP packets.

- Authentication by a RADIUS server

The LAC sends user names and passwords to the RADIUS server for authentication.

- Private IP address allocation

  The LNS can be deployed behind an intranet firewall to dynamically allocate and manage addresses.

- Reliability

  L2TP supports LNS redundancy. When the master LNS is unreachable, the LAC reestablishes connections with the backup LNS to improve the availability and fault tolerance of VPN services.

  L2TP application scenarios are NAS-initiated VPN, automatic LAC dial-up, and client-initiated VPN.

- NAS-initiated VPN

  A PC user dials up to the LAC using PPPoE, and the LAC initiates a request for establishing a tunnel to the LNS over the Internet. The LNS assigns an IP address to the user. The LAC proxy or both the LAC proxy and the LNS can authenticate the user. After the L2TP user goes offline, the tunnel is automatically removed to save network resources. This networking mode applies to the scenario in which users in branches initiate connections to the headquarters but do not frequently access the headquarters.

  Multiple enterprises can share a LAC to connect their branches to their headquarters. The LAC connects to multiple LNSs, and each LNS connects the headquarters of an enterprise.

  In L2TP over IPSec, packets are encapsulated through L2TP and then IPSec. L2TP is used to authenticate users and assign IP addresses, and IPSec ensures security. In this way, L2TP over IPSec integrates the advantages of the two VPN technologies.

- Automatic LAC dial-up

  A permanent L2TP connection is established between a LAC and an LNS. The connection between the client and LAC is an IP connection.

  The user can configure a permanent L2TP connection between a LAC and an LNS. The LAC establishes a permanent L2TP tunnel with the LNS by a local user name. The connection between the user and the LAC is an IP connection.

  This networking mode applies to the scenario where users in branches frequently access the headquarters. Users in branches can be directly connected to the headquarters, without user name authentication. The LAC provides L2TP services for multiple users in branches to prevent demanding dial-ups. The LNS authenticates only the LAC. Therefore, if a user at a branch can access the LAC, the user can access the headquarters without being authenticated, which is a security risk. To improve security, you can perform a second authentication over users on the device.

- Client-initiated VPN

  The client that supports L2TP dial-up can initiate a request for establishing a tunnel to the LNS, and the request does not need to pass through a LAC. The user can initiate a request for establishing a tunnel to the LNS, and the request does not need to pass through an independent LAC. The LNS assigns an IP address to the user. The LNS sets up a tunnel for each remote user. Therefore, the LNS configuration is more complex in client-initiated VPN than in NAS-initiated VPN. One advantage of client-initiated VPN is that users on the move can set up VPN connections anywhere using their mobile devices.

  In the client-initialized VPN scenario, mobile workers access servers at the headquarters for mobile working.

In L2TP over IPSec, packets are encapsulated through L2TP and then IPSec. L2TP is used to authenticate users and assign IP addresses, and IPSec ensures security. In this way, L2TP over IPSec integrates the advantages of the two VPN technologies.

Enhancement

None.

Dependency

None.

6.4 GRE

Availability

This feature has been introduced since V100R001.

Summary

The Generic Routing Encapsulation (GRE) protocol encapsulates the packets of certain network-layer protocols to transmit encapsulated packets by the protocol of another network layer. GRE is a Layer-3 tunneling technology.

Benefits

- Enables local networks with multiple protocols to transmit traffic through a single-protocol backbone network.

  GRE encrypts less used a protocol into a more universal protocol, such as from IPX to IP, and transmits the encrypted protocol in the backbone network.

  IPSec encrypts only unicast packets, but not multicast packets. Therefore, you can use GRE to encapsulate multicast packets, such as routing protocol, voice, and video packets into unicast packets and then IPSec to encrypt the packets. GRE and IPSec interworking improves transmission security of multicast data in tunnels.
- Expands the network whose hop count is restricted.

  Some network protocols do not support many hops, such as RIP. If the hop count between the two PCs exceeds 15, the PCs cannot communicate. The GRE tunnel hides certain hops, expanding the scope of the network.
- Implements the VPN across the WAN.

  If two subnets reside in different cities. The two subnets form a trans-WAN VPN through the GRE tunnel.

  The GRE VPN does not protect data and is rarely used.

Description

The GRE protocol encapsulates the packets of certain network-layer protocols to transmit encapsulated packets by the protocol of another network layer. GRE is a Layer-3 tunneling technology. A GRE tunnel is a virtual point-to-point connection that transmits encapsulated data packets.

The two ends of the GRE tunnel are tunnel interfaces which encapsulate and decapsulate data packets. The tunnel interface that sends encapsulated packets is called the tunnel source interface, and the one that receives these packets on the peer end is called the tunnel destination interface.

- Encapsulation

1. The USG receives an IP packet, and an IP module processes the packet.
2. The IP module checks the destination address in the packet header to determine how to forward this packet. If the packet is destined for the other end of the GRE tunnel, the IP module sends the packet to the tunnel interface.
3. The tunnel interface receives and adds a GRE packet header in encapsulation, and the IP module processes the packet.
4. The IP module encapsulates the GRE packet using a new IP packet header. The source address is the address of the tunnel source interface, and the destination address is the address of the tunnel destination interface. Then the IP module forwards the encapsulated IP packet from the WAN interface (tunnel source interface) based on the destination address and routing table.

- Decapsulation (in a reverse order)

5. The USG receives an IP packet and checks the destination address. If the destination is the USG and the protocol ID in the IP packet header is 47 (indicating GRE packet), the USG removes the IP packet header and sends the packet to a GRE protocol module.
6. The GRE protocol module checks the checksum and key fields, removes the GRE header, and sends the packet to the IP module.
7. The IP module forwards this packet.

- GRE security options

  To enhance the security of the GRE tunnel, the GRE protocol allows users to set the authentication keyword (or key) of the tunnel interface for end-to-end authentication. RFC1701 defines the key and checksum fields of a GRE header as follows:

8. If the Key Present bit is set to 1, the two ends implement keyword authentication on the packet. The packet passes the authentication only when the authentication keywords on both ends are the same.
9. If the Checksum Present bit is set to 1, the checksum is valid. The sender calculates the checksum based on the GRE header and payload, adds the checksum to the packet, and sends the packet to the peer end. The recipient calculates the checksum of the received packet and compares the calculated one with the one in the packet. If the two are the same, the recipient removes the GRE header and sends the packet to the IP protocol module. If the two are different, the recipient discards the packet.

Enhancement

None.

Dependency

None.

6.5 BGP/MPLS VPN

Availability

This feature has been introduced since V100R001.

Summary

Border Gateway Protocol (BGP)/Multiprotocol Label Switch (MPLS) VPN is a Layer 3 virtual private network (L3VPN) that employs BGP to advertise VPN routes and MPLS to forward VPN packets on the backbone networks of service providers.

Benefits

The MPLS technology combines the flexible IP routing and convenient asynchronous transfer mode (ATM) label switching. MPLS adds a connection-oriented control plane into the connectionless IP network to facilitate the management and operation of IP networks.

Therefore, the MPLS VPN that adopts 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.

BGP focuses on controlling route spread and choosing the optimal route instead of finding and computing routes. VPN uses a public network to transmit VPN data, and the public network uses Interior Gateway Protocol (IGP) to find and compute routes. To construct the VPN, it is critical to control route advertisement and select the best route between PEs.

BGP uses TCP as the transport-layer protocol (port 179), improving the protocol reliability. VPN routes between two PEs with the USG in between can be exchanged through BGP.

BGP carries any information added to routes. The information serves as the optional BGP attribute. If a USG does not know these attributes, it forwards them transparently, which facilitates the transmission of VPN routes among PEs.

During route updates, BGP sends only the updated routes, reducing the bandwidth for route transmission and making it possible to transmit a large number of VPN routes on the public network.

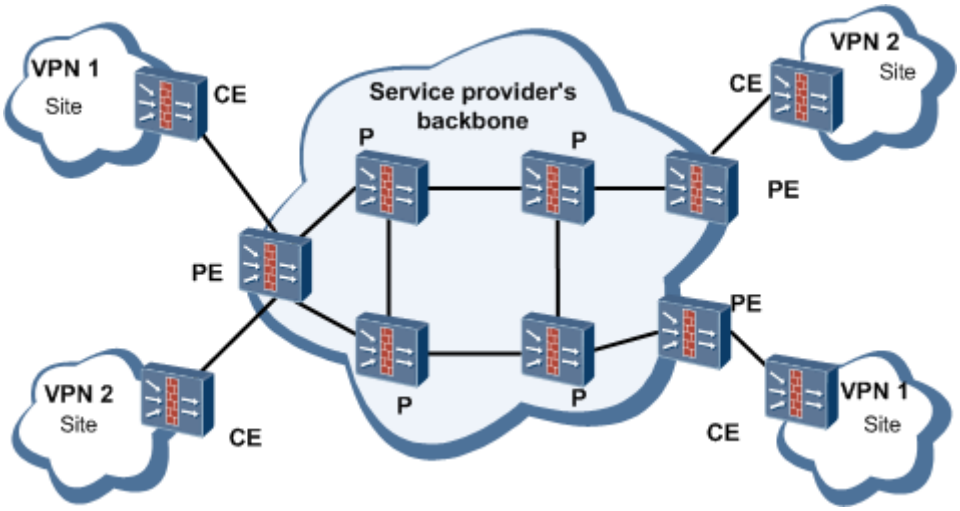
As an EGP, BGP better applies to the implementation of the VPN across carriers' networks.

Description

- Model

  The model is shown in the following figure:

Figure 6-3 BGP/MPLS VPN model



The basic model of BGP/MPLS VPN consists of the Customer Edge (CE), Provider Edge (PE), and Provider (P).

- CE: indicates the device at the border of a customer's network. A CE can be a router, switch, or host that is directly connected to the network of the Service Provider (SP) through an interface. In normal cases, a CE cannot perceive the existence of a VPN and is not required to support MPLS.
- PE: indicates the device at the border of an SP's network and is directly connected to the CE. On MPLS networks, all VPN-related processing is performed on the PE, which poses high requirements on the performance of the PE.
- P: indicates the backbone device on the SP's network and is not directly connected to the CE. The P needs to support only basic MPLS forwarding and does not maintain VPN-related information.

  The SP manages the PE and P, and the user manages the CE unless the user entrusts the management right to the SP.

  One PE can access multiple CEs, and one CE can connect to multiple PEs of one or multiple SPs.

  On a BGP/MPLS VPN, the USG works as a PE and supports L3VPN.
- Basic concepts
- Site

  Site indicates a group of IP addresses with connectivity, which can be realized without the SP' network. Sites are not connected through the backbone network
- VPN

  You can configure policies and divide multiple sites connected to one SP's network into multiple sets. Only sites in a set can access each other across the SP's network. This set is called a VPN.
- VPN instance

  Each VPN has multiple instances for private forwarding information. The instance is called VPN instance. In the VPN service, multiple interfaces connecting to the network may have the same IP addresses. You can bind the VPN instance to an interface to implement independent routing and forwarding between VPN instances.

You can bind a VPN instance to an interface on the local gateway and configure Route Distinguisher (RD) for each VPN instance. On the peer gateway, you can also bind the same instances to interfaces. You can configure internal route in the VPN instance and establish an independent routing table for each VPN instance. Each routing table has the routing information to destination addresses within the VPN instance.

When the local gateway forwards a packet, the packet carries the RD and destination address of the VPN instance. The peer gateway receives the packet, locate the destination device by the RD and destination IP address, and forwards the packet to the related VPN instance, resolving IP address overlap issue among multiple VPNs.

- Operating principle
  - VRF

    Independent routing tables maintained by the PE include public network and VPN routing and forwarding (VRF) tables. The routing and forwarding table on a public network include the routing information between all PEs and P routers. The VRF table includes the routing information accessible for local VPN users, and the information among multiple VRF instances is independent.

    PEs and CEs can exchange the routing information through EBGP, OSPF, RIP, or static routes.
  - VRF routing distribution

    We must exchange VPN routing information between PEs to keep VPN connected. The VPN router has an independent address space. Multiple VPNs may overlap their addresses. Therefore, we cannot exchange VPN routing information on the SP public network.

    The PE router converts the route to a VPN-IPv4 route by adding an RD, sets the next hop to itself, adds a private network label and RT attribute, and forwards the route to all PE neighbors.
  - Public network label allocation

    The PE and P routers learn the next-hop addresses of BGP neighbors using the backbone network IGP. The PE and P routers run LDP, allocate labels, and establish the label switched path (LSP) channel.

    A label stack forwards packets. Outer labels indicate how to reach the BGP next hope with inner labels indicating the VRF that an outbound interface of a packet belongs to.

  An MPLS node forwards labels by outer label.
  - Packet forwarding

    The CE sends a packet to the connected VRF interface. The PE searches routes in the local VRF table for the next-hop address of the public network and private network label,

    Adds the private label to the packet, searches the next-hop address in the label forwarding information base (LFIB) on a public network, adds the public network label, and sends the packet to the MPLS for forwarding.

    The PE forwards the packet the LSP. The last but one device removes the outer public network label and delivers the packet to the destination PE device.

    The PE identifies the outbound interface and next hop based on the inner private label, removes the private label, and forwards the packet to the CE based on the VRF.

Enhancement

None.

Dependency

None.

6.6 DSVPN

Availability

This feature has been introduced since V100R001.

Summary

Dynamic Smart VPN (DSVPN) is a technology to establish a data forwarding channel dynamically between spokes in the hub-and-spoke network model.

Benefits

- Benefits for carriers

  Meet carriers' requirement for low latency and high performance.
- Benefits for users

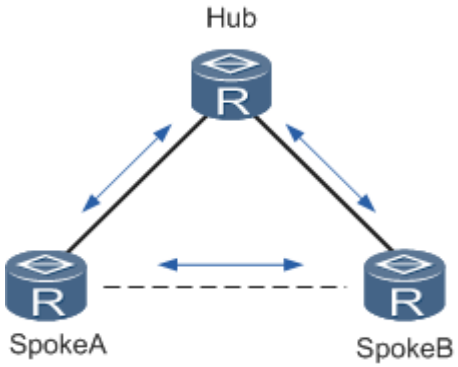
  Forward service data directly between branches, reducing forwarding delay and improving performance and efficiency.

Description

- Traditional hub-and-spoke network model

  In the traditional hub-and-spoke network mode, the data traffic locates between a spoke and the hub. If SpokeA sends traffic to SpokeB using the IPSec technology, the hub receives and decrypts the data from SpokeA, and encrypts and sends the data to SpokeB, consuming much hub resources and causing delay. To resolve the issue, the DSVPN technology establishes a data forwarding channel dynamically between spokes.

Figure 6-4 Traditional hub-and-spoke network model



- Route deployment

The next hop of a spoke must be another spoke instead of the hub to establish an IPSec channel between the two spokes for direct communication. The route deployment solutions are as follows:

- Configuring static routes between spokes

  Configure static routes on the source spoke with the destination address set to the destination spoke subnet and next hop set to the protocol address of the Multipoint GRE (MGRE) tunnel interfaces.

- Learning routes from spokes

  Enable the dynamic routing protocol for routing learning between a spoke and the hub and between spokes. Connect all spokes to one logical interface on the hub for direct learning between spokes. Disable split horizon for distance-vector routing protocols, such as RIP, for direct advertisement between spokes. There is no need to disable split horizon for OSPF, because OSPF is a link-state routing protocol and does not involve split horizon.

NOTE

In split horizon, the RIP does not advertise a route back through the interface from which the route was learned to neighboring devices.

- Configuring the aggregation route on a spoke only to the hub

  Learning routes between spokes proposes high requirements for spoke router capacity and performance. In a large deployment scenario, this solution requires high performance of spoke routers. On a spoke, you can set only the default forwarding routes from the spoke to the hub to direct all outgoing traffic for the destination spoke to the hub. When the hub forwards spoke traffic, the hub identifies whether the traffic goes within a VPN. If yes, the source spoke initiates a Next Hop Resolution Protocol (NHRP) request to the destination spoke. The destination spoke sends an NHRP reply, carrying the destination subnet information. Then the source spoke sends packets to the destination spoke again through a direct channel between the two spokes.

- Point-to-multipoint (P2MP) GRE
- GRE overview

  Generic Routing Encapsulation (GRE) is used to encapsulate the packets of certain network-layer protocols. Therefore, encapsulated packets can be transmitted on the IPv4 network.

- MGRE tunnel interface

  Similar to a loopback interface, MGRE tunnel interface is a P2MP logical interface to implement DSVPN.

Similar to GRE tunnel interfaces, the MGRE tunnel interface contains the following elements:

Source IP address: indicates the packet source IP address. For the network that transmits encapsulated packets, the source IP address of the tunnel is the IP address of the interface that sends the encapsulated packets.

IP address of the tunnel interface: indicates a 32-bit IP address used on the Internet, consisting the network code and host ID. The network code identifies a network, while the host ID identifies a device on the network. The IP address of the tunnel interface has the same meaning as the IP address of the GRE tunnel interface.

MGRE tunnel interfaces are not same as the GRE tunnel interfaces, and the difference is as follows:

Destination address: The destination address of the GRE tunnel interface is specified manually, while the destination address of the MGRE tunnel interface is from the NHRP. A P2MP GRE interface has multiple GRE tunnels connected to multiple GRE peer devices.

Tunnel type: The type of MGRE tunnel is P2MP GRE.

Restriction

The MGRE tunnel interface does not support keepalive detection.

- NHRP

  NHRP resolves how a source spoke obtains the Non-Broadcast Multiple Access (NBMA) next hops to a destination spoke on an NBMA network.

  The resolution process of NHRP addresses is as follows:

  Learning routes from spokes

1. All spokes on the network initiate registration requests to the configured hub.
2. The hub records the mapping between protocol addresses and NBMA addresses based on the registration requests and sends acknowledgments to spokes.
3. The source spoke receives acknowledgments and sets the status of the hub to **Active**.
4. Spokes learn routes on the spoke subnet using static or dynamic routing protocols and set the next hop to the peer spoke.
5. When a source spoke forwards IP packets, the spoke searches routes based on the destination address in IP packets. If the NGRP NBMA address does not exist in the IP packets, the spoke sends an NHRP address request to the destination spoke.
6. An intermediate equipment forwards the passerby NHRP address request.
7. The destination spoke constructs an NHRP reply and returns the mapping between protocol addresses and NBMA addresses on the destination subnet.
8. The source and destination spokes have complete NBMA address information for direct communication.

   Configuring the aggregation route on a spoke only to the hub

1. All spokes on the network initiate registration requests to the configured hub.
2. The hub records the mapping between protocol addresses and NBMA addresses based on the registration requests and sends acknowledgments to spokes.
3. The source spoke receives acknowledgments and sets the status of the hub to **Active**.
4. Pokes learn routes on the spoke subnet using static or dynamic routing protocols and have aggregation routes only to the hub.
5. When a source spoke forwards IP packets, the spoke searches routes based on the destination address in IP packets and forwards packets to the hub.
6. The hub identifies whether the inbound and outbound interfaces forwarding packets are in the same DSVPN. If yes, the hub forwards packets to the destination spoke and sends an NHRP redirect message to the source spoke to trigger the initiation of the NHRP request from the source spoke.
7. The source spoke receives the NHRP redirect message and sends the NHRP address request to the destination spoke.
8. The hub forwards the NHRP request to the destination spoke.
9. The destination spoke sends an NHRP reply to the source spoke, carrying the mapping between protocol addresses and NBMA addresses on the destination subnet.
10. The source spoke refreshes its NHRP mapping table based on the NHRP reply.
11. The source and destination spokes have complete NBMA address information for direct communication.

NOTE

You can select not to enable IPSec in the DSVPN deployment. To enable IPSec and protect the GRE traffic, inform the local device of the peer IP address to establish the IPSec tunnel.

If the IPSec tunnel is **Up** or **Down**, notify NHRP. NHRP selects packet forwarding routes based on the IPSec tunnel state.

- DSVPN reliability

  In the DSVPN deployment, all spokes are connected to the hub. If the hub is faulty, connection between spokes cannot be established. We can use the redundancy deployment of the hub to improve the DSVPN reliability.

  Each spoke registers on the NHRP server of the active and standby hubs. If the active hub is down, the standby hub works as the forwarding proxy for NHRP packets.

Enhancement

None.

Dependency

None.

6.7 SSL VPN

Availability

This feature has been introduced since V100R001.

Summary

Benefits

Description

Enhancement

None.

Dependency

None.

6.8 Certificate

Availability

This feature has been introduced since V100R001.

Summary

Benefits

Description

Enhancement

None.

Dependency

None.

7 Route

7.1 Policy-based Routing

Availability

This feature has been introduced since V100R001.

Summary

Using policy-based routing (PBR), the USG selects routes based on the customized policies but not the routing table and forwards packets based on more attributes, such as the inbound interface, source and destination security zones, source and destination IP addresses, user, service, and application. This selection adds flexibility to packet forwarding control.

Benefits

- More flexible route selection

  You can specify that multiple traffic select different routes for diversified management purposes, such as QoS requirement, VPN topology, or link expense. For example:

  User-specific routing: The specified users or user groups can access the Internet only through the specified links. For example, user group A has a higher permission and can use high-speed Internet services. User group B has a lower permission and access the Internet through a low-speed link.

  Application- and protocol-specific routing For example, the traffic of voice and video applications is forwarded to the high-bandwidth link, while the traffic of data applications is forwarded to the low-bandwidth link.

Description

To forward packets, the USG looks up the routing table and forwards the packets based on the destination address. This mechanism provides only the destination address-based forwarding service, but not differentiated service.

Using PBR, the USG selects routes based on the customized policies but not the routing table and forwards packets based on more attributes, such as the inbound interface, source and destination security zones, source and destination IP addresses, user, service, and application. This selection adds flexibility to packet forwarding control. PBR takes priority over but does not take place of the routing table mechanism. PBR provides guidance for forwarding the traffic of certain services.

PBR selects traffic and specifies the forwarding outbound interface or next-hop IP address based on policy settings, such as the inbound interface, source and destination security zones,

source and destination IP addresses, user, service, and application. The USG forwards the traffic matching the policy to the specified next hop and the traffic not matching the policy based on normal routing.

Enhancement

None.

Dependency

None.

8 Reliability

8.1 Hot Standby

Availability

This feature has been introduced since V100R001.

Summary

To prevent single-point failures, you can deploy two devices for hot standby. When one device goes faulty, service traffic can be smoothly switched to the standby device.

Benefits

- Prevents single-point failures

  The USG supports the active/standby mode. The active device processes services, while the standby device backs up the configuration and state information of the active device. When the active device goes faulty, service traffic can be smoothly switched to the standby device, ensuring service continuity.

- Improves throughput

  The USG supports the active/active mode. Two active devices process services and balance load using an external router. The two devices back up each other. When one device goes faulty, service traffic can be smoothly switched to the other device.

Description

With the popularity of network applications and the exponential bandwidth growth, a short network interruption may severely compromise services and lead to great losses. Therefore, high availability becomes a crucial factor in network construction.

To prevent single-point failures, you can deploy two devices for hot standby. When one device goes faulty, service traffic can be smoothly switched to the standby device with intranet and Internet users not aware of the network fault.

- Active/standby and active/active backup

  Active/standby backup

  In active/standby mode, the active device processes services, and the standby device stays in idle state. If an error occurs on the interface or link of the active device or the active device is faulty, the standby device becomes active and takes over services.

Active/standby backup prevents single points of failure, enhancing network availability. Therefore, active/standby is usually deployed at the access point of key services, such as the access point to the Internet or to a bank's database server.

Active/active (load balancing)

Load balancing means that two devices work in active/active mode and each processes part of services. When one device is faulty, the other device takes over all the services.

Two USGs share traffic using the balancing device. When you plan the network topology, ensure that the total traffic load of two devices does not exceed the processing capability of either device.

Both devices process services, which improves packet forwarding efficiency and eases the load on a single device.

- Data backup

  The USG needs to back up configuration and state information between the active and standby device. The configuration information refers to the data configured by users, including all service configuration data, such as user settings and policy settings. The state information refers to the service data created while the USG is running, such as session table.

  The USG has real-time and batch backup based on the backup time. In real-time backup, the USG backups change of configuration or state immediately. For example, if a user delivers configurations and selects real-time backup, sessions are backed up in real time upon the creation. In batch backup, the host synchronizes all configuration or state information to the standby device upon new access or restart of the standby device.
- State monitoring and switchover mechanism

  The USG monitors active and standby device state and processes the switchover using the heartbeat information and state advertisement.

  If a host finds itself faulty, such as a link fault, it notifies the standby device for switchover.

  If a standby device finds the heartbeat loss, the device implements immediate preemption and takes over the service.

  The USG hot standby function monitors the following states: interface state (physical interface, subinterface, Eth-trunk, and VLAN), link health check result, and BFD result.

Enhancement

None.

Dependency

None.

8.2 IP-Link

Availability

This feature has been introduced since V100R001.

Summary

IP-Link automatically detects reachability of the links indirectly connected to the device.

Benefits

The physical link check detects only links directly connected to the device without detecting all links. The device cannot detect the faults of links not directly connected to the device.

The IP-Link detects all link connectivity to avoid service interruption because of the faults of links not directly connected to the device.

Description

The IP-Link detects link connectivity by sending detection packets to the destination address. If no response packet is received within the specified interval (three seconds by default), the device regards that the link is faulty and performs further link-related operations. If three successive response packets are received within the specified period through the link that was considered to be faulty, the device regards that the link recovers and performs further operations of link recovery.

The USG supports the ICMP echo request and ARP request. If the IP address of the USG detection interface and the destination host IP address are on the same network segment (multiple Layer-2 devices can be deployed between the USG and destination host), the ARP request can be used for detection. If not, the ICMP echo request can be used for detection, and the destination host must be able to receive the ICMP echo request and respond to the request.

The USG IP-Link can be used in the following scenarios:

- Hot standby

  If the USG works in hot standby, you can use the IP-Link to monitor the links of peer devices not directly connected to the USG. If a link is faulty and may affect services, you can trigger the switchover of the active and standby USG for service continuity.

- Static route

  If multiple static routes exist between the USG and destination address, you can use the IP-Link to monitor the reachability of each static route. If the check detects a link fault, the USG adjusts its static routes to ensure the highest priority and reachability of every used link for service continuity.

- PBR

  PBR cannot sense the reachability of the next hop and the link of the default next hop. When the next hop or the link of the default next hop is unreachable, setting the next hop or the default next hop may cause packet forwarding failures.

  Interworking PBR with IP-link solves the previous problem and improves the flexibility of PBR applications and the dynamic network scenario sensation of PBR. The check monitors the reachability of the links of the next hop and the default next hop. If links are normal, PBR takes effect. If a link is faulty, PBR does not take effect.

Enhancement

None.

Dependency

None.

8.3 BFD

Availability

This feature has been introduced since V100R001.

Summary

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

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.

Benefits

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

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

Description

- Current link detection mechanism

  To reduce the adverse impacts on services and promote the network availability, communication faults between neighboring devices must be identified rapidly, so that countermeasures can be taken timely for service continuity. Currently, the following fault detection mechanisms are available:

  Hardware detection: For example, Synchronous Digital Hierarchy (SDH) alarming can rapidly identify faults, but it is not available on all media.

  Slow Hello mechanism: The detection duration of the routing protocol Hello mechanism is at the second level. For high-speed data transmission such as the transmission at the Gigabit rate, the long detection duration that longer than 1s may cause serious data loss. For sensitive services such as voice, the detection duration is not acceptable.

  Other detection mechanisms: Dedicated detection mechanisms may be provided by different protocols or device vendors. If a network has devices from multiple vendors, these detection mechanisms are difficult to implement.

- BFD purposes

  BFD overcomes the limitations of current detection mechanisms. The BFD purposes are as follows:

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

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

- BFD implementation principle

In BFD mechanism, a BFD session is established between two systems, and BFD control packets are transmitted periodically. If one system does not receive any BFD control packet in a certain period, the path is regarded faulty.

BFD control packets are encapsulated in UDP packets for transmission. At the beginning of a session, two systems negotiate with each other through the parameters (such as the session identifier, minimum expected packet sending/receiving interval, and BFD session status on the local system) in BFD control packets. After the negotiation, BFD control packets are transmitted along the path on the basis of the negotiated packet sending/receiving interval.

To realize quick detection, the packet sending/receiving interval is regulated to the microsecond level in the BFD draft. Limited by the processing capability, BFD only reaches the millisecond level on the devices of most vendors, and is further converted to the microsecond level during internal processing.

- Interworking of BFD and OSPF

  Link faults or topology changes may cause the router to recalculate routes. To improve the network availability, the convergence time of routing protocols must be shortened. Link faults can never be completely prevented. Therefore, it is more practical to enhance the fault identification rate and report faults to routing protocols in time.

  In interworking, BFD is associated with OSPF. Through BFD, link faults can be quickly identified and reported to OSPF, and OSPF can quickly respond to the topology change.

  BFD can accelerate the convergence rate of OSPF from the second level to the microsecond level.

- Interworking of BFD and static routing

  Static routes are manually configured by administrators. Static routing has no detection mechanism. If a fault occurs on the network, the administrator should handle it.

  After a static route is bound to the static BFD session, the static route can dynamically change its status upon the change of BFD session status.

  If the BFD session detects the interface fault (the status changes from Up to Down), BFD reports the faults to the system. The system deletes this route from the IP routing table and switches the service traffic to the standby link. If the BFD session is established successfully (the status changes from Down to Up), BFD reports the change to the system. The system adds this route to the IP routing table and switches the service traffic to the active link.

- Interworking of BFD and FRR

  Fast ReRoute (FRR) is a technology to minimize link fault impact on services. If a physical layer or data link later is faulty, the BRR reports the fault to upper-layer routing system and transfers packets in a standby link.

  On a traditional IP network, if the transfer link is faulty, the status of the physical interface on a router changes to Down. If the router detects the fault, the router reports the upper-level routing system for update and calculates routes again. The duration from a fault occurrence to the route convergence (reselect a reachable route) takes a few seconds.

  The duration is intolerable for services that are sensitive to packet loss and delay because this duration results in service interruption. For example, Voice Over IP (VoIP) services can be interrupted up to the microsecond level. IP FRR ensures that the forwarding system detects faults and takes measures quickly to recover services.

  However, IP FRR must be triggered by a fault detection mechanism, such as BFD, to take effect.

- Interworking of BFD and PBR

PBR is a mechanism that selects routes based on the customized policy rather than forward packets by searching the IP table based on the destination addresses of IP packets. The PBR can be used for security or load balancing.

PBR supports the route selection based on the information, such as the source IP address and packet type. If meeting certain conditions (matching ACL rules), packets are processed for forwarding according to configurations (such as egress and next-hop IP addresses, and default egress and next-hop IP addresses).

PBR cannot sense the link reachability. If the link is unreachable, packet forwarding may fail.

Interworking PBR with BFD solves the issue and improves the flexibility of PBR applications and the dynamic network environment sensation of PBR. Configure static routes to interwork with BFD. BFD monitors the availability of the next hop or egress link and dynamically determine the availability of PRB based on the status of the BFD session.

- Interworking of BFD and DHCP

  For network availability, some enterprises use the dual-uplink networking. The active link is the DHCP access link. The enterprise egress gateway works as the DHCP client and obtains the IP address from the DHCP server. The standby link is the PPPoE access link.

  The egress gateway works as the DHCP client and cannot sense the DHCP link reachability. If the link is faulty, service traffic cannot be switched to the standby link quickly, resulting in service interruption.

  Interworking of DHCP and BFD resolves the issue. If the BFD session is associated on the DHCP client, the availability of the DHCP link is dynamically determined based on the status of the BFD session

Enhancement

None.

Dependency

None.

9 Basic Security

9.1 Security Filtering Policy

Availability

This feature has been introduced since V100R001.

Summary

The security filtering policy allows some traffic through the USG and denies some traffic based on packet or traffic classification.

Benefits

- Secures the intranet

  By default, a user can allow specified traffic through the USG and deny the other traffic to secure the intranet.
- Controls permissions

  The security filtering policy can limit accessible resources to users to control permissions.
- Classifies traffic

  The traffic classification technology in the security filtering policy is the basis of other security policies. The technology performs security check, such as bandwidth control and IPS and AV implementation over specified traffic.

Description

The security filtering policy allows some traffic through the USG and denies some traffic based on packet or traffic classification.

The USG classifies traffic by source or destination domain, protocol number, source or destination IP address, service type, application type, and user group or user name.

You can configure the valid period of the security filtering policy on the USG. For example, an employee cannot play games or access entertainment websites in working hours.

Enhancement

Compared to the traditional firewall, the USG implements wider filtering. Besides the network layer filtering implemented by the traditional firewall, the USG filters by user name, user group, and application type.

Dependency

None.

9.2 Bandwidth Control Policy

Availability

This feature has been introduced since V100R001.

Summary

The USG manages and controls bandwidth by source address, destination address, source security zone or incoming interface, destination security zone or outgoing interface, service, user, or application.

Benefits

- Guarantees bandwidth

  When a link is busy, the device can ensure the availability of sufficient bandwidth for key services transmitted over the link.
- Limits bandwidth

  A limit can be set on the amount of bandwidth that non-key services are allowed to use.
- Limits connections

  Limiting the number of connections of a service saves session resources and prevents the service from overusing bandwidth resources

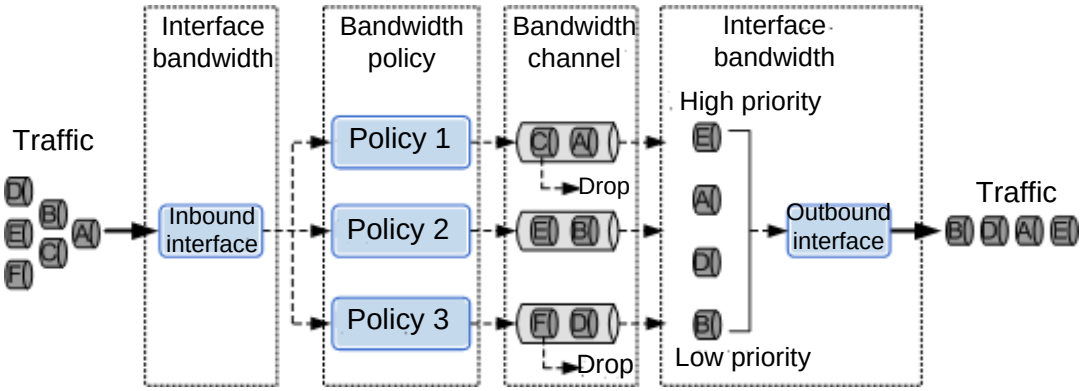
Description

The USG manages and controls bandwidth by source address, destination address, source security zone or incoming interface, destination security zone or outgoing interface, service, user, or application. The USG guarantees and limits bandwidth and limits connections.

- Bandwidth management procedure

  The USG implements bandwidth management using the bandwidth policy, bandwidth channel, and interface bandwidth. The bandwidth policy defines the managed objects and actions and references a bandwidth channel. The bandwidth channel defines the bandwidth resources that the managed objects can use, and the resources are to be referenced by the bandwidth policy Interface bandwidth defines the actual bandwidth on the inbound interface and outbound interface. If a traffic congestion occurs in outbound direction, the USG uses the queuing mechanism to ensure orderly traffic transmission.

Figure 9-1 Bandwidth management procedure



The bandwidth management process on a USG is as follows:

1. On the inbound interface, the traffic is limited by the interface bandwidth and processed based on the bandwidth policy.
2. The USG enforces traffic policies to match and classify traffic for multiple bandwidth channels.
3. The bandwidth channel discards traffic that exceeds the predefined maximum bandwidth and limits the number of connections for one service. The bandwidth channel marks the traffic priority for follow-up queuing mechanism.
4. On the outbound interface, the USG forwards traffic based on the limitation of interface bandwidth. If the traffic requires bandwidth higher than the interface bandwidth, the USG uses the queuing mechanism to ensure orderly traffic transmission based on packet priorities.

- Bandwidth channel

  The traffic that matches the bandwidth policy enters the bandwidth channel. A bandwidth channel defines bandwidth resources, which is the basis of bandwidth management.

  Bandwidth channels divide physical bandwidth resources into multiple logical bandwidth resources. The bandwidth channel uses multiple parameters to describe and control bandwidth resources, such as overall guaranteed bandwidth and maximum bandwidth, maximum bandwidth for each IP address or user, limitation on the number of connections, and priority remarking. The bandwidth channel also implements sharing of bandwidth resources.

  Overall guaranteed bandwidth/maximum bandwidth: The overall guaranteed bandwidth is the minimum available bandwidth assigned by a traffic channel to traffic that enters the traffic channel. Similarly, the overall maximum bandwidth is the maximum available bandwidth assigned by a traffic channel to traffic that enters the traffic channel. After the traffic enters the bandwidth channel, the USG compares the traffic with the guaranteed and maximum bandwidth. If the traffic is lower than the guaranteed bandwidth, the traffic can be forwarded at the outbound interface. If larger, the traffic is discarded. If the traffic is higher than the guaranteed bandwidth but lower than the maximum bandwidth, the traffic competes for bandwidth resources with the same type of traffic that is processed using other traffic channels. The bandwidth channel with higher priorities uses the remaining bandwidth resources. The USG discards packets that fail to obtain bandwidth resources.

  Maximum bandwidth for each IP address or user: In addition to the guaranteed and maximum bandwidth, the maximum bandwidth for each IP address or user can be specified in a traffic channel to implement fine-grained bandwidth limit. The USG can

specify bandwidth for each IP address or user or specify that all online users share the bandwidth.

Limitation on the number of connections: You can set a limit to the total number of connections in a traffic channel. You can also set a limit to the number of connections for each source IP address or user to implement fine-grained limit.

Priority remarking: The USG supports the priority remarking function in the bandwidth channel. You can change the DSCP priority to a new value if the traffic matches the specified bandwidth policy matching conditions, so that the upstream and downstream devices of the USG can distinguish the traffic based on the remarked DSCP priorities.

Bandwidth sharing: If multiple traffic flows exist in the bandwidth channel, the bandwidth channel assigns bandwidth resources dynamically. If a traffic flow does not use bandwidth resources, other traffic flows can borrow the idle resources. If a traffic needs network resources, the traffic can preempt bandwidth resources. Bandwidth sharing cover the following scenarios:

- Traffic flows matching the same bandwidth policy can share bandwidth resources.
- If multiple bandwidth policies reference the bandwidth channel by policy sharing, traffic flows matching bandwidth policies can share bandwidth resources.
- Traffic flows matching multiple child policies in parent and child policy can share bandwidth resources.

- Bandwidth policy

  Bandwidth policies define the traffic types to be managed and how to implement bandwidth management. A bandwidth policy references a traffic channel. When a USG determines that traffic matches a specified bandwidth policy, the USG allocates bandwidth resources to the traffic based on the traffic channel referenced by the bandwidth policy.

  A bandwidth policy is a set of bandwidth rules with each rule consisting of conditions and actions. The USG uses conditions to match packets. The conditions include source security zone/inbound interface, destination security zone/outbound interface, source address, destination address, user, application, service, time segment, and packet priority. Actions refer to the processing methods that the USG uses for packets, including **car** and **no car** for the management over traffic that matches conditions. If the action is set to **car**, a bandwidth traffic is referenced in a bandwidth policy and determines management measures. If the action is set to **no car**, the traffic that matches conditions are not managed.

- Interface bandwidth

  Configure interface bandwidth to specify the bandwidth resources for both inbound and outbound traffic on USG interfaces.

  When the USG works as an enterprise egress gateway, the bandwidth that the enterprise purchases from carriers is generally less than the physical bandwidth capacity of the USG outbound interface. If maximum available bandwidth is not set on the outbound interface, the bandwidth may exceed the available bandwidth on the outbound interface. As a result, traffic congestion occurs, and packets may be discarded.

  You can set the maximum outbound bandwidth to less than or equal to the bandwidth purchased by the enterprise. If traffic exceeds the maximum available bandwidth on the outbound interface, the USG considers that traffic congestion occurs and uses the queuing mechanism to ensure that key services with higher priorities are forwarded preferentially.

You can also set the maximum inbound bandwidth. Therefore when the USG receives traffic from other devices, the USG can limit the inbound traffic.

Enhancement

None.

Dependency

None.

9.3 ASPF

Availability

This feature has been introduced since V100R001.

Summary

During communications, some applications need to establish multiple transport-layer connections, such as the FTP control connection and data connection. The control connection transmits control commands, and the data connection uploads and downloads files.

The data connection is established based on the IP address and port information negotiated in the control connection. The data connection is established dynamically, and its direction, IP address, and port may be different from those of the control connection. Therefore, it is difficult for the security filtering policy to control the traffic. If the traffic is not managed, services may be affected. The USG detects the application-layer data in the control connection and automatically obtains information and establish session entries to ensure normal communications, which is called Application Specific Packet Filter (ASPF).

Benefits

The USG provides ASPF to resolve packet payload in the control channel through the multi-channel protocol and resolve the channel negotiation information. The ASPF temporarily enables the policies that allow the pass of data channel based on the negotiated IP address and port of the data channel. Therefore, after the control channel of the multi-channel protocol passes through the USG, the data channel passes through the USG.

Description

ASPF is a state-based packet filter mechanism applied to the application layer. ASPF can detect the application-layer protocol session packets that attempt to pass through the device. By maintaining the status of sessions and checking the information about the protocols and port numbers of session packets, the device can normally forward special packets.

ASPF is imported for the forwarding of multi-channel protocols. These protocols automatically negotiate certain random ports during communications, but in the case of strict security policies, the packets sent from the random ports cannot be normally forwarded. To resolve the issue, the system can use ASPF to resolve the application-layer data, identify the port numbers negotiated by these protocols, and open the corresponding access rules.

In the NAT scenario, NAT ALG is also enabled.

Enhancement

None.

Dependency

None.

9.4 URPF

Availability

This feature has been introduced since V100R001.

Summary

A router receives packets, obtains the destination address, and searches the forwarding table based on the destination address. If the table is found, the router forwards the packet. If not, the router discards the packet. After unicast reverse path forwarding (URPF) obtains the source address and inbound interface, URPF searches the interface for the source address in the forwarding table and checks the interface. If the interface does not match the inbound interface, the source address is regarded disguised, and the packet is discarded. Therefore, URPF can prevent malicious attacks that modify source IP addresses.

Benefits

URPF can resolve network security issues caused by address spoofing.

Description

After URPF obtains the source address and inbound interface, URPF searches the interface for the source address in the forwarding table and checks the interface. If the interface in the forwarding table is the same as the inbound interface of the packet, the source address is regarded disguised, and the packet is discarded. Therefore, URPF can prevent malicious attacks that modify source IP addresses.

The USG implements URPF in the following two modes:

- Strict mode

  After the USG receives a packet, the USG searches the forwarding table based on the source IP address. If the forwarding table cannot be found, the USG discards the packet. If the forwarding table is found, the USG checks all matched outbound interfaces in the forwarding table. If the inbound interface of the packet is the same as the outbound interface in the forwarding table, the packet passes the URPF check. If not, the packet is discarded.

  In strict mode, URPF is highly secure but can be used only in symmetric route environment. URPF in asymmetric route environment may make incorrect judgment in strict mode.
- Loose mode

After the USG receives a packet, the USG searches the forwarding table based on the source IP address. If the forwarding table cannot be found, the packet is discarded. If the forwarding table is found, the packet passes the URPF check and can be forwarded.

URPF in loose mode does not compare the outbound interface in the forwarding table and the inbound interface of the packet and can be used in asymmetric route environment.

Enhancement

None.

Dependency

None.

9.5 NetStream

Availability

This feature has been introduced since V100R001.

Summary

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

Benefits

- Charging

  NetStream provides refined data, including IP address, packet number, byte number, time, ToS, and application type for the charging based on the occupation of resources, such as lines, bandwidths, and time segments. ISPs can use the data to implement flexible charging policies based on the time, bandwidth, application, and service quality. Enterprise customers can use the data to calculate expenses or allocate costs to effectively utilize resources.

- Network planning and analysis

  NetStream provides key information for network management tools to optimize network design and planning and to obtain optimal network performance and reliability through low operating costs.

- Network monitoring

  NetStream delivers the real-time network monitoring function. The RMON, RMON-2, and information flow-based analysis technology vividly illustrate the traffic mode of a single router and the entire network and provide advanced fault detection, effective troubleshooting, and fast issue solving capabilities.

- Application monitoring and analysis

  Through NetStream, the detailed information about network applications can be obtained. For example, network administrators can view the percentages of the traffic of web, FTP, Telnet, and other well-known TCP/IP applications. According to the information,

Internet content and service providers can plan and allocate network and application resources to meet users' requirements.

- Traffic anomaly detection

  By analyzing flows, NetStream detects abnormal traffic on networks in real time, such as various network attacks. In addition, NetStream secures network by sending alarms on the network side and interworking with devices.

Description

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

NetStream is a statistics technology based on network traffic information, collects classified statistics on the communications traffic and resource usage on networks, and monitors and manages networks on the basis of services and resources. Output NetStream data can be applied to multiple aspects, including network management and planning, enterprise accounting, department-based charging, ISP compilation billing, data storage, and commercial data collection.

NetStream includes the NetStream Data Exporter (NDE), NSC, and NetStream Data Analyzer (NDA). The NDE collects traffic and sends the detailed information about the traffic to the NSC. The NSC collects, stores, filtering, and the statistics, filters, and aggregates the information and sends the statistics to the NDA. The NDA performs further aggregation and sorting and display the data in figures. The result displayed by the NDA provides reference for network charging, networking planning, network monitoring, application monitoring, analysis, and fault location. The USG is an NDE device.

On networks, the IP network is connectionless. Therefore, the communications between different types of services are implemented through a group of IP packets sent from one terminal to another. Actually, these IP packets form the data flow of a network service. Most data flows are temporary, intermittent, and bidirectional. NetStream identifies different flows based on the 7-tuple form constructed by the destination and source IP addresses, destination and source port numbers, protocol numbers, ToS, and input and output interfaces, and collects data statistics on these flows. The USG serving as the NDE periodically sends the obtained statistics to the NSC for further processing. The NSC sends the statistics to the NDA to analyze data and form reports. Charging and network planning are implemented based on the reports.

The USG collects data and outputs the statistics.

- Data collection

  If NetStream is enabled on the interface, the system stores NetStream information in the interface information form. If every packet is involved in the NetStream establishment and counting, the device performance especially high-speed interface will be affected greatly. Therefore, you need to select packets passing through the interface and send the information to NetStream for processing. Lower collection ratio affects less on devices.

- Flow output

  NetStream identifies different flows based on the 7-tuple form constructed by the destination and source IP addresses, destination and source port numbers, protocol numbers, ToS, and input and output interfaces, and collects data statistics on these flows. If the flow ages out, the flow information is sent to the NSC. The output methods include original flow and aggregated flow.

  Original flow output: The system collects the aged NetStream flow information, constructs UDP packets, and sends the packets to the NSC. After the NSC obtains

detailed flow information, the NSC processes the flow records flexibly. However, the CPU usage of the network bandwidth and device is increased. In addition, a large storage capacity is required to store the information, which puts much pressure on the device.

Aggregated flow output: The system collects, classifies, and combines the aged NetStream flow information and generates the aggregated information. If the system timer ends, the aggregated flow is sent in UDP packets. Aggregation of original flows can decrease the network bandwidth, CPU usage, and storage media capacity.

Enhancement

None.

Dependency

None.

9.6 Attack Defense

Availability

This feature has been introduced since V100R001.

Summary

The attack defense function of the USG detects network attacks and protects the hosts in intranet against possible attacks.

The USG can defend Distributed Denial of Service (DDoS) attacks and traditional single-packet attacks.

Benefits

The attack defense function of the USG helps large enterprises and data centers defend against common single-packet attacks and DDoS attacks. Deploy the USG on the intranet egress and enable attack defense, so that the USG can forward normal traffic and block attacks, ensuring the normal operation of the intranet server and PC and smooth response to service requests.

Description

The USG attack defense function divides attacks into the single-packet attack, scanning attack, and DDoS attack based on the attack method. The USG takes different defense methods for multiple attacks.

- Single-packet attack

  In the single-packet attack, a few malformed or special packets are used to launch attacks. Or the single-packet attack causes system corruption and target network congestion when the target host processes the packets, or detects the status of the target host or network for follow-up attacks.

  The USG supports the following single-packet attacks: IP spoofing, IP fragment anomaly, Teardrop, Smurf, Ping of Death, Fraggle, WinNuke, Land, TCP flag bit exception, and

ARP spoofing. The USG performs detailed check over the packet content and allows legitimate packets through.

Special packet control attacks do not directly bring damages to network devices. The attacker probes the network topology by sending special packets, preparing for further intrusion. Special control packet attacks, including oversized ICMP packet control, ICMP unreachable packet control, ICMP redirect packet control, Tracert, IP source routing packet control, IP route record packet control, and IP timestamp packet control. In a scenario that these control packets are not required, you can enable the USG attack defense functions to deny these control packets.

- Scanning attack

  As potential attack behaviors, scanning attacks do not directly bring damages to network devices. Such attacks are network probe behaviors before real attacks. Scanning attacks include address scanning and port scanning attacks.

  Address scanning: The attacker uses ICMP packets (such as the ping or Tracert command) or TCP/UDP packets to initiate connections to certain IP addresses. Based on the response packets, the attacker can determine which target systems are alive and connected to the target network.

  Port scanning: The attacker probes the network topology through port scanning and locates the ports currently enabled on the target and specify the attack mode. In port scanning attacks, the attacker uses the Port Scan software to initiate connections to a series of TCP or UDP ports on a wide range of hosts. According to the response packets, the attacker can determine whether these hosts provide services through these ports.

  The USG recognizes scanning attacks based on statistics. The USG collects the number of probing on the target IP address or port within a specified period from a source. If the number exceeds the predefined threshold, the USG considers that the source is launching scanning attacks and denies packets from the attack source.

- DDoS attack

  The DDoS attack interferes with or even blocks normal network communications by overloading the target network. An attacker submits massive requests to the target server or network to overload the server or congest the network. Therefore, legitimate users' access to the server to network is denied. The DDoS attack is a flood attack.

  The USG defends against the following attacks: SYN flood attacks, UDP flood attacks, ICMP flood attacks, HTTP flood attacks, HTTPS flood attacks, DNS flood attacks, and SIP flood attacks. With anti-DDoS, the USG detects attacks and prevent attacks.

1. Attack detection

   The attack detection checks whether a protected host or network is suffering from DDoS attacks based on statistics and determines whether to enable the anti-DDoS function. If the number of requests that a network or host receives within a specified period exceeds a threshold, the USG considers that a DDoS attack occurs and enables the anti-DDoS function.

2. Attack defense

   If the DDoS attack occurs, the USG enables the anti-DDoS function. The attack defense denies the attack traffic without affecting normal traffic passing through the USG. The USG uses the following anti-DDoS technologies based on attack and protocol characteristics:

   Source probing technology: The USG detects the source IP addresses of the request packets by checking whether the source IP address can respond to the detection packet correctly. The USG forwards packets from a real source IP address and discards packets from a forged source IP address to prevent attacks. The source probing technology can

prevent the SYN flood, HTTPS flood, DNS request flood, DNS reply flood, and SIP flood attacks.

Signature technology: A flood attack uses specified attack tools to launch attacks, and packets generated by the tools have characteristics. The USG learns the characteristics of detected attack packets and saves them as fingerprints. Once a packet matches a fingerprint, the packet is discarded. The signature technology can prevent UDP flood and UPD Fragment flood attacks.

Redirection technology: The USG redirects any received request to its own source. If the source re-initiates the request, the request is then forwarded to the original destination. After the re-initiated request arrives, the USG verifies the source and redirects the request to its original destination. The redirection technology can prevent the HTTP flood attack.

Traffic limiting technology: If the device cannot identify the attack traffic and normal traffic using all methods, or the normal access traffic exceeds the upper limit, the device discards the exceeding packets to protect the target host or network. The traffic limiting technology can be the last protection mechanism in anti-DDoS.

Enhancement

None.

Dependency

None.

9.7 Terminal Security Interworking (Interworking with the TSM)

Availability

This feature has been introduced since V100R001.

Summary

With the development of networks and the prevalence of firewalls, the main sources of the network security risks on enterprises gradually transfers from external networks to internal networks. The proposal of the TSM solution can eliminate the hidden security problems brought by internal network terminal users.

The USG acts as the security access control gateway (SACG) in the TSM solution, isolates different areas, and controls the access permissions of terminal users.

Benefits

Terminal security interworking can solve the following issues:

- Illegitimate terminals and unauthorized terminals access the service system in the following cases:

1. Non-private terminal devices access the intranet.
2. Illegitimate users use enterprise devices to access the intranet.

3. Legitimate users access unauthorized network resources.

- Insecure terminals spread viruses.
- Terminals are of a large number, systems are complex, and employee violations cannot be monitored.

Description

With the development of networks and the prevalence of firewalls, the main sources of the network security risks on enterprises gradually transfers from external networks to internal networks. The proposal of the TSM solution can eliminate the hidden security problems brought by internal network terminal users.

- TSM solution operating principle

  The TSM solution divides the network into the following domains:

  User domain: includes all terminal devices accessing the intranet, such as the desktops, laptops, and personnel on business trip, regional offices, and partners using the Internet for access.

  Network domain: includes network devices for traffic forwarding. The network domain bears service traffic and interconnects networks. The SACG is deployed in this domain

  Pre-authentication domain: The domain can be accessed by terminal devices before authentication is complete. The domain implements authentication, authorization, policy management, and patch delivery on terminals and users. Most components of the TSM solution are deployed in this domain.

  Controlled domain: The domain can be accessed by terminals only after authentication is complete. The controlled domain includes the post-authentication and isolation domains. The isolation domain can be accessed by terminal users who pass identity authentication but not authorization. Resources that help users eliminate security risks, such as the patch server and antivirus server, are deployed in the isolation domain. The core resources of an enterprise are deployed in the post-authentication domain. Therefore, terminals and users can access the security zones corresponding to their permissions only after passing authentication and authorization.

The working procedure of the TSM solution is as follows:

4. The terminal accesses the network and initiates an authentication request.
5. The SACG forwards the authentication request to the TSM Controller and prevents terminals that do not pass the authentication and authorization from accessing the post-authentication domain.
6. The TSM system implements the check on permissions and terminal security. If security vulnerabilities exist on the terminal, the TSM system grants the device the permission of accessing the isolation domain, so that the terminal can download the patch or virus library. After security vulnerabilities are repaired, the TSM system determines whether to allow the terminal to access the post-authentication domain and which post-authentication domain to be accessed.
7. The TSM system delivers the user access control policy that is generated for the terminal to the SACG.
8. The SACG generates a forwarding policy according to the received policy and determines whether to allow the terminal to access the post-authentication domain through the SACG.

- SACG operating principle

  The USG works as the SACG in the TSM solution and controls network access permissions. In the TSM solution, the TSM system configures access control policies for

various users automatically delivers the policies to the USG, requiring no manual configurations.

The principle for the TSM server to deliver the access control policy to the SACG is as follows:

9. The TSM system uses roles to manage user permissions with each role for a controlled domain and an access control list (ACL) in the TSM system. After the USG enables TSM interworking, the USG obtains ACLs for all roles from the TSM system. There is one default role for all access users, and the role can allow an unauthenticated user to access the pre-authentication domain.
10. After accessing the network, the terminal initiates an authentication request through the SACG to the TSM server. After the terminal passes authentication, the TSM server sends the information about the IP address and role of the terminal to the SACG.
11. According to the information of the ACLs delivered by the TSM server, the SACG creates a source IP address monitoring table and records the relationships among the IP addresses, roles, role permissions, and available resources.

- SACG deployment modes

  The USG provides in-line and off-line modes.

12. In-line mode

    In in-line mode, the device is directly connected to the original network of the user in serial mode. The USG accesses the user network as a Layer-2 or Layer-3 forwarding device.

13. Off-line mode

    The intranet exists when you use the TSM function. The terminal user and service system are connected through a core forwarding device (such as a Layer-3 switch or a router). If you replace the forwarding device with the SACG for deploying the TSM system, the intranet needs to be re-constructed and routes need to be re-learned. To avoid the issue, you can deploy the SACG in off-line mode. In addition, the off-line mode prevents SACG faults from causing network interruptions.

    In off-line mode, the SACG is connected to the original router or switch as an off-line device. You can configure the redirection or PBR on the router or switch to forward traffic from the router or switch to the SACG. The SACG interworks with the TSM server to identify the permission for the user of the traffic and processes the traffic. If the traffic is allowed through the SACG, the SACG sends the traffic to the router or switch for forwarding.

    This networking directly adds the SACG and TSM server group on the original network without changing the original network structure. As the traffic passes the SACG in only one direction, the requirement on the load balancing of the SACG is low.

Enhancement

None.

Dependency

None.

9.8 Location Awareness

Availability

This feature has been introduced since V100R001.

Summary

The USG provides location awareness to identify the traffic source and destination location, such as country, area, and city, by source IP address and destination IP address.

Benefits

- Traffic analysis based on location

  The USG analyzes the packet location, collects statistics and analyzes the traffic based on location, and generates the traffic report and threat report based on the location.
- Policy configuration based on location

  You can configure security policies based on location to limit the Internet users' access to enterprise resources. For example, you can allow users in city 1 to access the server resources and deny the users in city 2 from accessing the server resources.

Description

Carriers allocate different IP address segments to multiple areas and enterprises. Location information can be obtained by searching the IP address, which is location awareness.

With the location awareness technology, the USG can perform the following functions:

- Policy configuration based on location

  This function helps user and traffic management based on the region. With location awareness, the USG can configure the security filtering policy, bandwidth control policy, authentication policy, and audit policy.
- Traffic statistics and analysis based on location

  The traffic report generated by the USG based on location displays the traffic ranking by traffic size. The ranking also displays the source and destination location of the traffic that passes through the USG within the searched period. You can click the location name to view the traffic statistics about the IP address in the location.
- Threat statistics and analysis based on location

  The threat report generated by the USG based on location displays the threat ranking by number of threats. The ranking also displays the source and destination location of all traffic that passes through the USG within the searched period. You can click the source location name to view the attacker statistics in the location. You can click the destination location name to view the attack target statistics in the location.

Enhancement

None.

Dependency

None.

10 Application-Layer Security

10.1 SA

Availability

This feature has been introduced since V100R001.

Summary

Traditional firewalls identify applications and performs policy control by port. If an application uses an ephemeral port for communications, the application may bypass the firewall detection.

Service Awareness (SA) of the USG analyzes the packet payload deeply and identifies the real application type of the traffic.

Benefits

- Application-based policy control

  The USG uses SA and performs policy control based on the SA result and supports application-based security policy detection, traffic control policies, and PBR.
- Application-based traffic analysis

  With SA, the USG can analyze and generate the traffic report based on applications.

Description

The USG SA analyzes packet signatures and interaction procedure deeply and identifies applications and protocols correctly.

- Combination of multiple identification methods

  The USG SA uses a combination of multiple identification methods for correct application and protocol identification. The USG can identify common protocols, such as HTTP, and other applications using common protocols, such as Facebook and Webmail.
- Predefined rule base

  The USG SA uses a rule base for application identification. To meet diversified requirements for application identification, the rule base can be updated online.

  Huawei provides a predefined rule base that can identify over 5000 common protocols and applications, which can meet most users' requirements.

- User-defined rules

  The USG SA also provides the user-defined rule function for application identification to meet diversified requirements.

  For special protocols and applications, users can configure rules based on the IP address, port, and content matching and add scenarios that predefine rules cannot identify.

Enhancement

None.

Dependency

None.

10.2 IPS

Availability

This feature has been introduced since V100R001.

Summary

The USG intrusion prevention system (IPS) can perform application-layer analysis and detection over the traffic that passes through the USG based on SA and identify and defense against multiple network attacks.

The USG IPS can detect threats, such as the Trojan horse, worm, and Botnet, and attacks, such as SQL injection and XXS, based on vulnerabilities.

Benefits

- Secures the network

  The IPS can prevent network attacks effectively and secure intranet hosts and servers.
- Defense against attacks in real time

  The IPS supports online update of the signature database in real time to prevent new attacks.

Description

- Deployment modes

1. Off-line deployment

   The off-line mode can detect traffic without any defense or cleaning, which does not affect the traffic.
2. Online detection deployment

   The online detection mode can detect traffic without taking any defense actions. This mode modifies only QoS and TTL without discarding or modifying packets.
3. Online defense deployment

   The online defense mode can support detection and cleaning mode and take defense actions, such as discarding, modification, and traffic limiting, over detected threats.

- Features

4. Predefined rules for detection

   The USG provides predefined rules, including policies defending against common vulnerability attacks, Botnets, Trojan horses, worms, SQL attacks, and XXS attacks. Users can generate a signature set by selecting the object, severity, operating system, protocol type, and threat type and customize predefined rules. Users can also define exception signatures to exempt unsuitable signatures.

5. User-defined rules for detection

   Users can define rules, including objects and rules to meet added IPS requirement. The rules include judgment conditions for decoding fields.

6. Association detection

   The system predefines the threat association detection that indicates the relationship of basic threat events. Defining the association can help the system discover deeper threats.

7. IPS anti-evasion

   Attackers may evade the IPS to attack network devices or servers. The IPS anti-evasion can ensure detection integrity and correctness.

8. IPS supporting IPv6

   The IPS supporting IPv6 feature supports detection of threats in IPv6 data.

9. IPS supporting virtualization

   With the IPS supporting virtualization, users can use multiple virtual systems with independent configurations, policies, and log systems. A user can see only one virtual systems, as if the user is using the physical device exclusively.

10. Engine and signature database update

    The USG provides the online and offline update of engines and signature databases to prevent new threats on the live network.

Enhancement

None.

Dependency

None.

10.3 AV

Availability

This feature has been introduced since V100R001.

Summary

The USG antivirus (AV) feature can perform application-layer detection over the traffic passing through the USG, analyze transmitted files, detect viruses, and block the transmission of virus infected files.

Benefits

The USG AV feature blocks the transmission of virus infected files and prevent damages to customer servers and PCs.

Description

The USG AV feature can perform application-layer detection over the traffic passing through the USG, analyze transmitted files, detect viruses, and block the transmission of virus infected files. The USG AV feature supports the following functions:

- Resolution of diversified application-layer protocols

  The USG AV feature supports the resolution of diversified application-layer protocols, analyzes transmission actions, and scan viruses in transmitted files.
- Identification of multiple file types

  The USG AV feature supports multiple file types, detects viruses in decompressed files, and identifies the real file type based on file content to prevent detection evasion by modifying the file name extension.
- Flow-based AV detection

  The USG AV feature supports flow-based AV detection, which is high in defense performance.
- AV detection virtualization

  With the IPS supporting virtualization, users can use multiple virtual systems with independent configurations, policies, and log systems. A user can see only one virtual systems, as if the user is using the physical device exclusively.
- Update of the virus signature database

  Update of the virus signature database can help users detect viruses on the live network. The update does not affect the AV detection.

Enhancement

Dependency

None.

10.4 Content Filtering

Availability

This feature has been introduced since V100R001.

Summary

The USG content filtering feature performs application-layer analysis over transmitted data in real time, detects and blocks application-layer content based on the predefined filtering policies to minimize risks caused by unauthorized files and sensitive content transmission.

Benefits

- Protects enterprises from losing confidential data.

  The risks caused by losing confidential data include brand reputation damage, violation penalties, economic loss, customer distrust, and competition disadvantages.

- Complies with laws and regulations.

  The content filtering feature filters data, generates detailed monitoring reports, and proves the compliance with internal rules and relative laws and regulations to enterprise audit personnel and other stakeholders.

- Improves enterprise productivity.

  Using emails, instant messages, blogs, or FTP servers to upload and download files improves the work procedure and efficiency but poses great threats on information security. Enterprises can configure content filtering policies to enable employees to transmit and access legitimate content securely and to limit behaviors that decrease productivity, such as accessing illegitimate websites, browsing blogs not related to work, microblogging, and posting in forums.

Description

The content filtering feature includes protocol content, file type, and file content filtering based on scanning and filtering objects.

- Protocol content filtering

  Some application-layer protocols carry information in the protocols, such as the web page content, forums, microblogs, and emails. You can configure policies to filter the protocol content.

  With SA, the USG can identify traffic using ephemeral ports for communications to prevent the evasion and misjudgment.

  The USG supports in-depth protocol decoding, such as decoding of multi-layer protocols, content decompression, and normalization, to prevent the application-layer evasion.

- File type filtering

  The file type filtering function can filter transmitted at the application layer by file type to prevent high-risky and confidential files from passing through the USG. The USG also supports filtering by file name extension and real file type.

  With filtering by real file type, the USG can identify the real type of transmitted files base on the file content to prevent evasion.

  The USG also supports decompression and filters decompressed files.

- File content filtering

  The USG can perform in-depth file content and filter file content to avoid sensitive information leakage and illegitimate information intrusion.

  With filtering by real file type, the USG can identify the real type of transmitted files base on the file content to prevent evasion.

  The USG also supports decompression and filters decompressed files.

  The USG normalizes the file content to prevent evasion using coding technologies.

- Keyword configuration

  The USG provides default filtering keywords, such as the bank card, credit card, Social Security number, and ID for content filtering.

  Users can define keywords, such as common character strings and regular expressions.

Enhancement

None.

Dependency

None.

10.5 HTTPS Traffic Defense

Availability

This feature has been introduced since V100R001.

Summary

With HTTPS traffic defense, the USG can analyze the HTTPS traffic content and defense the application layer after decryption to prevent the malicious traffic from evading USG detection using HTTPS.

The HTTPS traffic defense supports URL filtering.

Benefits

Application-layer detection and data filtering over encrypted HTTPS traffic can prevent malicious users from using HTTPS to transmit viruses, Trojan horses, and confidential information.

Description

For security, more and more applications use encryption channels, such as HTTPS. However, the encryption channels causes risks. For example, some applications can use the encryption channels to transmit viruses, Trojan horses, confidential information, or illegitimate information to avoid the firewall detection.

With HTTPS traffic defense, the USG can decrypt the HTTPS traffic that passing through the USG and perform the same security detection over the HTTPS traffic as the HTTP traffic. The HTTPS traffic defense includes the follows aspects:

- Work as an SSL proxy.

  The USG works as the SSL proxy to encrypt the HTTPS traffic, because the SSL traffic cannot be encrypted using listening. The USG works as an SSL proxy as follows:

1. The USG intercepts the SSL negotiation requests from the client, works as a server to negotiate with the client using its own certificate, and establishes an SSL tunnel with the client.
2. The USG initiates and establishes an SSL tunnel with the real server.
3. The USG forwards the client and server traffic as a transparent proxy server. The USG decrypts the received traffic from one tunnel end, performs application-layer detection, and delivers the encrypted traffic from the other tunnel end.

- Detect the application layer.

  After decrypting the SSL traffic, the USG can perform the same application-layer detection over the decrypted HTTPS traffic as the HTTP traffic. Because the HTTPS traffic becomes the HTTP traffic after decryption.

- Restrictions

4. To establish the SSL tunnel with the client, the USG certificate must be trusted by the client.
5. The USG cannot work as a proxy in scenarios where the server authenticates the client certificate.

Enhancement

Dependency

None.

11 Virtual Firewall

11.1 Virtual Firewall

Availability

This feature has been introduced since V100R001.

Summary

A firewall can have multiple virtual gateways with each virtual gateway regarded as an independent firewall device with different system resources, administrators, security policies, and user authentication data.

Benefits

- Improves flexibility.

  The USG has multiple logical firewalls with each virtual firewall for a department. Each virtual gateway has independent administrators, security policies, and user authentication data, which improves the USG management flexibility.
- Reduces costs.

  A physical USG can have multiple virtual firewalls, which reduces investment on firewall devices.

  A small enterprise can rent a virtual firewall to reduce costs.

Description

A firewall can have multiple virtual gateways with each virtual gateway regarded as an independent firewall device with different system resources, administrators, security policies, and user authentication data. The virtual gateway has the following functions:

- Configuration virtualization

  Each virtual firewall can have its own administrator for configuration management.

  Each firewall can configure independent security policies and user authentication policies.
- Resource virtualization

  The operation of virtual gateways requires resources. The USG can specify the interface, and VLAN and configure number of policies, allowed session specifications, and bandwidth specifications for each virtual firewall.

Enhancement

Dependency

None.

12 Acronyms and Abbreviations

Table 12-1 Acronyms and Abbreviations

Abbreviation	Full Name