

Overview of Cyber Security Certification



Foreword

- Before studying the HCIP-Security course, we need to learn about the course positioning and outline.
- In January 2022, China's Ministry of Industry and Information Technology released the *Competency Framework of Industrial Talents in network information security*, which standardizes the types and responsibilities of cyber security engineers. Accordingly, HCIP-Security certification is intended for security implementation engineers and security O&M engineers.
- In this course, we will learn the types and responsibilities of cyber security engineers, capability models for security implementation engineers and security O&M engineers, and the HCIP-Security course outline.

Objectives

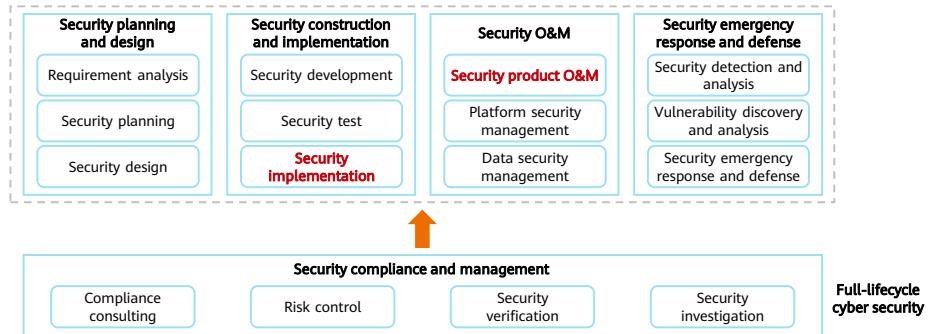
- On completion of this course, you will be able to:
 - Describe the position classification and responsibilities of cyber security engineers.
 - Describe the capability model for security implementation engineers.
 - Describe the capability model for security O&M engineers.
 - Understand the HCIP-Security course outline.

Contents

- 1. Capability Models for Cyber Security Engineers**
2. Cyber Security Certification

Major Directions of Cyber Security and Positions

- Cyber security engineers adopt security technologies, products, and services in various phases, such as planning and design, construction and implementation, operations and maintenance (O&M), and emergency response and defense. They are also responsible for full-lifecycle security compliance and management. In this way, information, information systems, and information infrastructure and networks are confidential, integral, and available, as well as well-protected from damages, changes, disclosures, or being excessively used due to unintentional, accidental, or malicious reasons.
- The following figure shows the full-lifecycle cyber security and the position directions of cyber security engineers.



4 Huawei Confidential

HUAWEI

- This course is intended for security implementation engineers and security O&M engineers.
- This section is written based on Competency Framework of Industrial Talents in network information security released by China's Ministry of Industry and Information Technology in January 2022.
- According to the assurance system of cyber security life cycle, the positions of the cyber security industry are mainly divided into five directions: security planning and design, security construction and implementation, security O&M, security emergency response and defense, and security compliance and management.
 - Security planning and design is the basic step in the whole cyber security life cycle. It involves comprehensive planning and designing of the security assurance system for the network system based on product and service security requirements, including security requirement analysis, security strategy planning, and security architecture design.
 - Security construction and implementation is a key step in the whole cyber security life cycle. It mainly refers to security development, test, and implementation based on security requirements, including security product development, basic security test, and onsite security implementation.

- Security O&M is an important step in the whole cyber security life cycle. After information, information systems, and information infrastructure and networks are delivered and used, security O&M personnel are deployed and tools are used, based on security framework, security policies, and mature O&M management system. Moreover, effective and efficient technical means are used to perform operation monitoring and security maintenance on assurance information, information systems, and information infrastructure and networks to ensure their security. Security O&M includes security product O&M, platform security management, and data security management.
- Security emergency response and defense is an important safeguard for the whole cyber security life cycle. It identifies, analyzes, and handles security threats to information, information systems, and information infrastructure and networks through security detection, vulnerability analysis, and defense technologies. It also collects cyber security information, and performs security analysis, proactively assesses the effectiveness of security protection measures through penetration attacks and attack and defense drills, continuously improves security protection measures, and quickly conducts emergency response when a security event occurs. Security emergency response and defense includes security detection and analysis, vulnerability discovery and analysis, and security protection and emergency response.
- Security compliance and management runs through the whole cyber security life cycle. It provides security compliance consulting, analyzes risks, provides solutions, and performs compliance supervision, risk control, and security assessment based on related laws, regulations, standards, and actual security requirements. It involves security compliance consulting, risk control, security assessment, and cyber security investigation.

Position Requirements for Cyber Security Talents

- Before introducing the capability models for security implementation engineers and security O&M engineers, we need to learn about the position requirements for cyber security talents.
- Cyber security talents should meet the following position requirements: comprehensive capabilities, professional knowledge, technical skills, and engineering practices.

Comprehensive capabilities	Professional knowledge	Technical skills	Engineering practices
<p>Behaviors and comprehensive qualities:</p> <ul style="list-style-type: none">• Self-study• Communication and coordination• Requirement and trend analysis• Insights into service scenarios...	<p>Necessary knowledge:</p> <ul style="list-style-type: none">• Basic theories• Relevant standards and specifications• Relevant laws and regulations• Theoretical knowledge and operational skills...	<ul style="list-style-type: none">• Professional knowledge• Use of profession tools	<p>Necessary experience:</p> <ul style="list-style-type: none">• Actual engineering• Project promotion

- This course focuses on the development of professional knowledge and technical skills.

Capability Model for Security Implementation Engineers

- Security implementation engineers and security O&M engineers mainly work in the security operation and maintenance phase.
- Security implementation engineers are responsible for the planning and design of the security implementation solutions and engineering implementation as well as formulation and compilation of the acceptance solutions, training solutions, and delivery documents. The requirements for professional knowledge and technical skills of security implementation engineers are as follows:

Professional knowledge	Technical skills
<ul style="list-style-type: none">• Master the current standards related to cyber security services.• Be familiar with the technical specifications and implementation processes of security attack and defense drills, penetration testing, security consulting, code audit, and emergency response in the cyber security service system.• Master security service rules and creation, and provide integrated and advanced security solutions for sophisticated service environments.• Be familiar with the basic knowledge related to cyber security services, and be familiar with the principles, deployment, and security assessment methods of mainstream security vendors' equipment.	<ul style="list-style-type: none">• Master skills such as port monitoring, analysis and detection of vulnerabilities, permission management, intrusion and attack analysis and tracing, website penetration prevention, and virus and Trojan horse prevention.• Be familiar with the configurations of cyber security devices.• Master basic commands and tools of the operating system and be familiar with common services.• Be familiar with system and application security protection, working principles of vulnerability scan, and cyber security technologies.• Be familiar with basic network principles, TCP/IP protocols, common protocols such as HTTP, FTP, and SNMP, and routine maintenance operations of switches and routers.

7 Huawei Confidential



- According to this slide, requirements on the professional knowledge and technical skills of implementation engineers are as follows:
 - Security standards: such as ISO27001. For details, see HCIA-Security certification.
 - Security construction rules and solutions: Implementation engineers need to fully know the implementation details of the security solutions.
 - Network principles and configurations of cyber security devices: deployment and configurations of cyber security devices should be mastered by implementation engineers and are also the key points of HCIA/HCIP-Security certification.
 - System and application security: Services are running on servers and operating systems. Therefore, system and application security should be taken into full consideration in security implementation.
 - Technologies and processes such as attack and defense drills and emergency response: The feasibility of routine O&M needs to be considered during security solution deployment.

Capability Model for Security O&M Engineers

- Security O&M engineers are responsible for performing security maintenance, security inspection, policy maintenance and management, configuration change, troubleshooting, and security analysis on servers, network devices, security products, and network information systems to eliminate detected threats and reduce security risks faced by enterprises.
- The requirements for professional knowledge and technical skills of security O&M engineers are as follows:

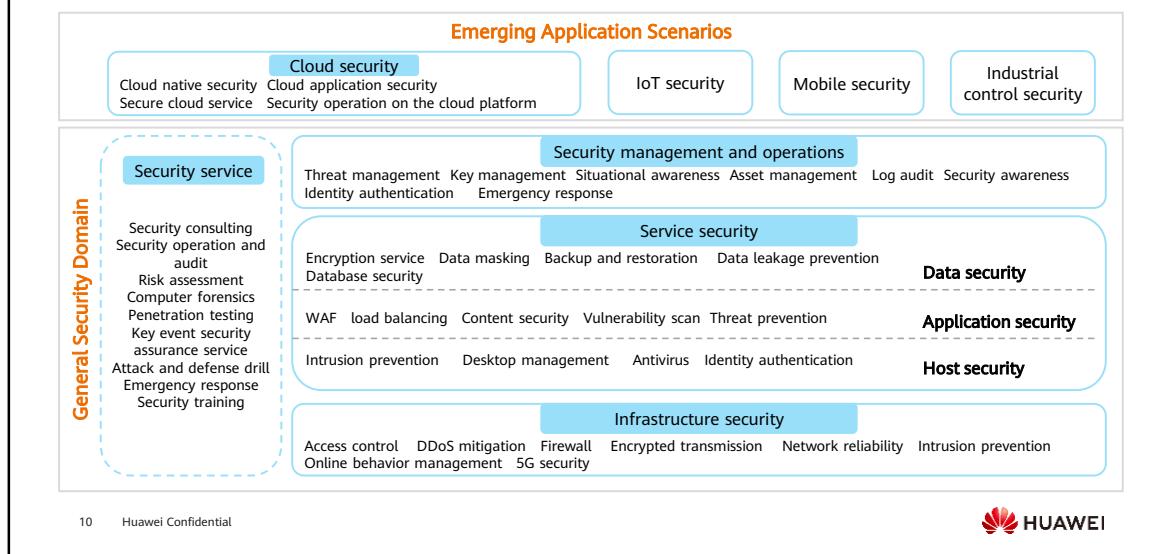
Professional knowledge	Technical skills
<ul style="list-style-type: none">• Master technical guides and standards related to security O&M.• Master common operation commands of operating systems and network devices.• Be familiar with the attack principles of common security vulnerabilities.• Be familiar with the processes and methods of security monitoring, security analysis, risk handling, and emergency response in security O&M.	<ul style="list-style-type: none">• Master O&M operations on common cyber security products, such as firewalls, IDS/IPS, and log audit.• Master network operation protocols such as TCP/IP.• Master the detection and protection principles of security vulnerabilities in common applications and operating systems, such as SQL injection, XSS, and privilege escalation vulnerabilities, and fix the vulnerabilities.• Be proficient in using operating systems such as Linux and Windows and database languages such as Oracle and MySQL.• Be familiar with common network monitoring methods.

- Security O&M engineers and security implementation engineers face similar requirements on professional knowledge and technical skills. Security implementation engineers focus on the deployment of security solutions, security devices, and functions. Higher requirements are exerted on O&M engineers in terms of troubleshooting, threat identification, and emergency response.
- Accordingly, security certification focuses on planning and design of cyber security solutions, implementation and construction, and O&M and optimization.

Contents

1. Capability Models for Cyber Security Engineers
2. **Cyber Security Certification**
 - Panorama of Cyber Security Concepts and Huawei Security Certification
 - HCIP-Security Course Outline

Panorama of Cyber Security Concepts



- The above figure shows common cyber security concepts in general security domain and emerging application scenarios.
 - General security domain: Any network involves security technologies, including infrastructure security, service security, security management and operation, and sometimes security services.
 - Infrastructure security: Security devices and their functions are used to ensure the security of the entire network, including protecting intranet services, network architecture, and facilities.
 - Service security: The security of services and bearer devices are to be ensured, including protecting hosts, applications on hosts, and background data.
 - Security management and operation: Any network requires security management, including administrative management regulations and technical management methods, such as security awareness cultivation and security situational awareness.
 - Security services: Security service providers provide security services for enterprises, such as risk assessment and attack and defense drills.
 - Emerging application scenarios: Feature-based protection is added based on general security technologies and service uniqueness. For example, in the cloud security scenario, cloud application security needs to be protected in addition to general security technologies.
 - This course applies to cyber security implementation engineers and O&M engineers, focuses on infrastructure security, and partially involves service security, and security management and operation.

Overview of Huawei Security Certification

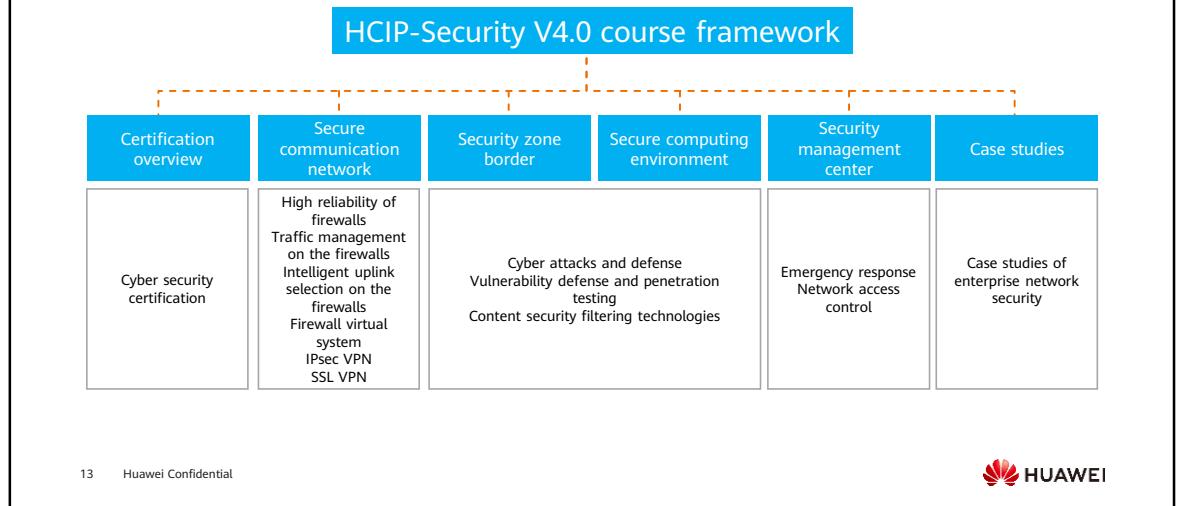
 <p>Enable learners to gain a deep understanding of defense skills, integrate enterprise security planning and design to help cultivate security architects.</p>	Everything in charge, building secure network solutions				 Expert Cyber security architect					
 <p>Focus on the four areas, give in-depth explanation based on products, focus on practice.</p>	Four areas, sharpening the mind <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 25%; padding: 5px;"> Secure communication network <ul style="list-style-type: none"> High reliability technologies Intelligent uplink selection on the firewalls VPN technologies Traffic management technologies </td> <td style="width: 25%; padding: 5px;"> Security boundary <ul style="list-style-type: none"> Cyber attack defense Firewall virtual system Content security and filtering </td> <td style="width: 25%; padding: 5px;"> Secure computing environment <ul style="list-style-type: none"> Application threat prevention Emergency response </td> <td style="width: 25%; padding: 5px;"> Security management center <ul style="list-style-type: none"> Access control </td> </tr> </table>				Secure communication network <ul style="list-style-type: none"> High reliability technologies Intelligent uplink selection on the firewalls VPN technologies Traffic management technologies 	Security boundary <ul style="list-style-type: none"> Cyber attack defense Firewall virtual system Content security and filtering 	Secure computing environment <ul style="list-style-type: none"> Application threat prevention Emergency response 	Security management center <ul style="list-style-type: none"> Access control 	 Professional Security implementation engineer Security O&M engineer	
Secure communication network <ul style="list-style-type: none"> High reliability technologies Intelligent uplink selection on the firewalls VPN technologies Traffic management technologies 	Security boundary <ul style="list-style-type: none"> Cyber attack defense Firewall virtual system Content security and filtering 	Secure computing environment <ul style="list-style-type: none"> Application threat prevention Emergency response 	Security management center <ul style="list-style-type: none"> Access control 							
 <p>Provide theoretical basis, enable beginners to improve security awareness, and learn about the technology framework of information security.</p>	Five modules, opening the security gate <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%; padding: 5px;">Concepts of cyber security</td> <td style="width: 20%; padding: 5px;">Basic network knowledge</td> <td style="width: 20%; padding: 5px;">Firewall basics</td> <td style="width: 20%; padding: 5px;">Intrusion prevention technologies</td> <td style="width: 20%; padding: 5px;">Encryption and decryption application</td> </tr> </table>				Concepts of cyber security	Basic network knowledge	Firewall basics	Intrusion prevention technologies	Encryption and decryption application	 Associate Security implementation engineer Security O&M engineer
Concepts of cyber security	Basic network knowledge	Firewall basics	Intrusion prevention technologies	Encryption and decryption application						
11 Huawei Confidential										

- HCIA-Security certification mainly applies to security implementation engineers and security O&M engineers. It is intended for people who are about to engage in or interested in related fields, such as students and new employees. After passing the certification, examinees prove that they have mastered the basic information security knowledge and related technologies (such as Huawei firewall technologies, encryption and decryption technologies, and PKI certificate system) on the small- and medium-sized networks. They are also capable of building information security networks for small- and medium-sized enterprises to ensure the security of networks and applications.
- HCIP-Security certification also mainly applies to security implementation engineers and security O&M engineers. After passing this certification, examinees prove that they have mastered Huawei cyber security technologies (including network architecture security, boundary security, application security, and endpoint security). They are also capable of designing, deploying, and maintaining cyber security architectures for medium- and large-sized enterprises, and are able to identify risks and respond to them promptly to ensure the security of enterprise information assets.
- HCIE-Security certification focuses on cyber security architects, and cultivates and certifies security experts with comprehensive capabilities in the design, deployment, and O&M of enterprise information security solutions. After passing this certification, examinees prove that they have mastered the latest security system architecture and best practices of security standards, and have comprehensive capabilities in the design, deployment, and O&M of information security solutions for medium- and large-sized enterprises. They meet enterprises' evolving requirements for network security and address increasingly diversified network security challenges.

Contents

1. Capability Models for Cyber Security Engineers
2. **Cyber Security Certification**
 - Panorama of Cyber Security Concepts and Huawei Security Certification
 - HCIP-Security Course Outline

HCIP-Security Course Framework



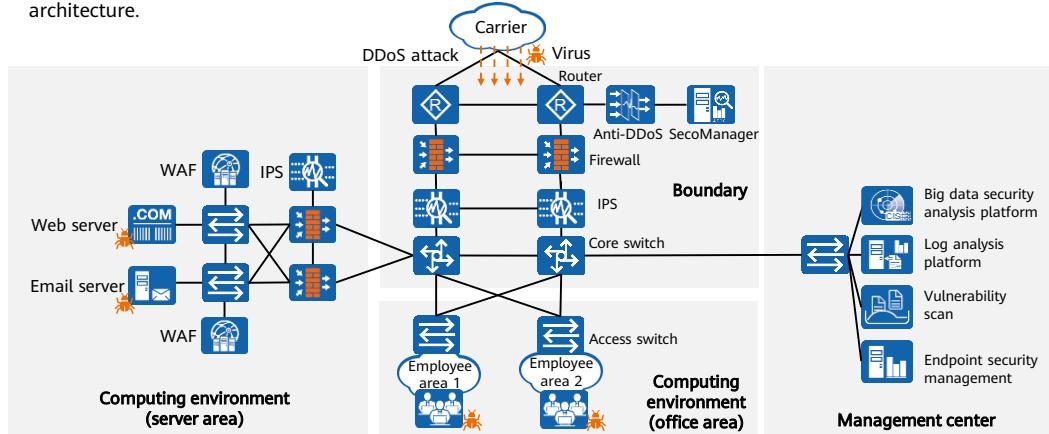
13 Huawei Confidential



- This course first describes the positioning and framework of HCIP-Security course based on "Overview of Cyber Security Certification".
- The high-level knowledge of Huawei cyber security solution is divided into four aspects: security communication architecture, security zone border, secure computing environment, and security management center. Based on the basic knowledge points of HCIA-Security, this course describes the technical details of Huawei cyber security solution.
- Finally, Huawei cyber security cases are used to systematically explain how security implementation engineers deploy security solutions and how security O&M engineers perform routine O&M.

Overview of Enterprise Network Security Threats

- An enterprise faces internal and external security threats. The following figure shows a typical enterprise network architecture.



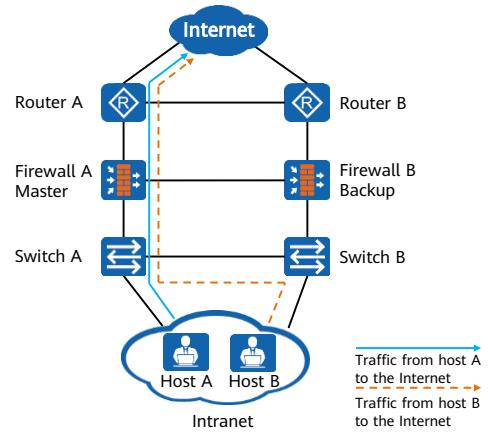
14 Huawei Confidential

HUAWEI

- Security threats to enterprise networks can be classified into the following types:
 - External threats: security threats from outside the enterprise network, such as DDoS attacks, viruses, Trojan horses, worms, network scan, spam, phishing emails, and web vulnerability attacks;
 - Internal threats: unreliable network structure, network without isolation, endpoint vulnerabilities, uncontrolled employee behavior, information security violation, information leakage, disordered permission management, and unauthorized access.
- Emerging security threats pose more and more security challenges to enterprises, and enterprise security requirements increase accordingly.

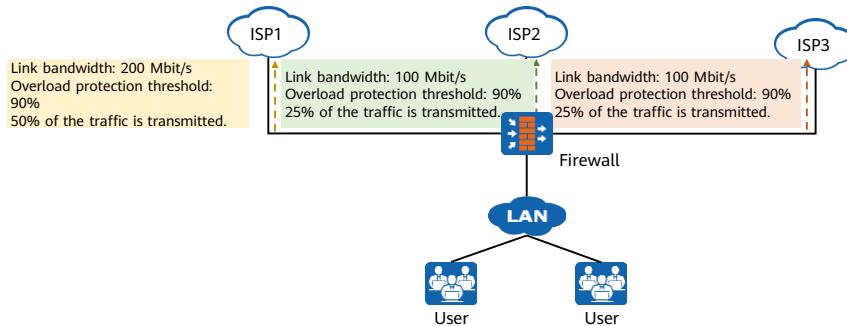
Communication Network Security Requirement - Device Redundancy

- The network architecture of the secure communication network needs to provide hardware redundancy for communication lines, key network devices, and key computing devices to ensure system availability. The devices include but are not limited to forwarding devices such as routers and switches as well as security devices such as firewalls, IPS, and Anti-DDoS.
- High reliability of firewalls is used as an example for security authentication. The HCIA-Security course describes the operating principles and service forwarding mechanism of firewalls in hot standby mode. The HCIP-Security course will introduce more networking and routine O&M operations of firewalls in hot standby mode.



Communication Network Security Requirement - Line Redundancy

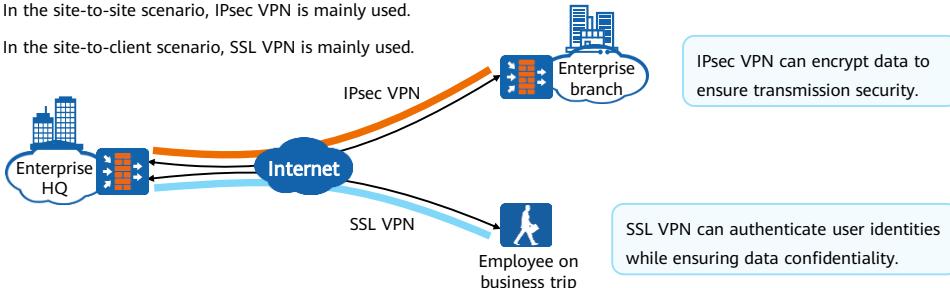
- Large- and medium-sized enterprises usually have multiple egress links, and firewalls typically serve as network egress devices. Egress devices usually select the optimal link based on routes or randomly select a link from equal-cost routes to forward traffic. However, the quality, bandwidth, and costs vary depending on links. Enterprises need to dynamically select the optimal path based on their requirements or properly distribute traffic to each link based on different proportions to improve link resource utilization and user experience.



Communication Network Security Requirement - Encrypted Transmission

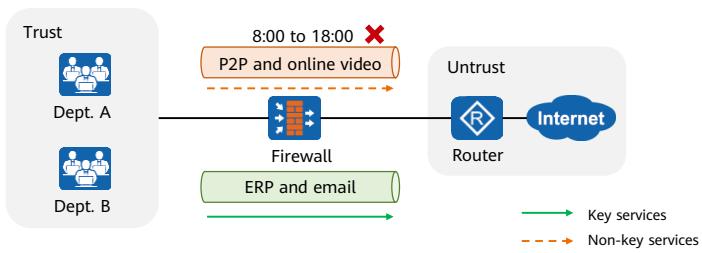
- There are two methods to prevent enterprise information from being stolen during transmission: private line transmission and encrypted VPN transmission. Private line transmission is applicable to communication between different organizations with high cost. Therefore, VPN encrypted transmission is commonly used on the live network.

- In the site-to-site scenario, IPsec VPN is mainly used.
- In the site-to-client scenario, SSL VPN is mainly used.



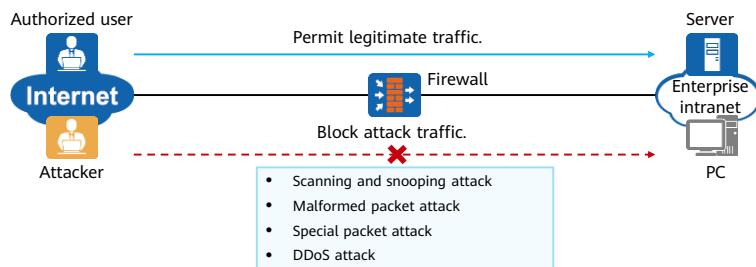
Communication Network Security Requirement - Bandwidth Management

- The network architecture of the secure communication network needs to ensure that the bandwidth for all services on the networks needs to be met during peak hours. Bandwidth management can be configured on the firewall to ensure the bandwidth for key services. In addition, quota control policies can also be configured on the firewall to manage users' Internet access traffic and duration, improving employees' work efficiency.



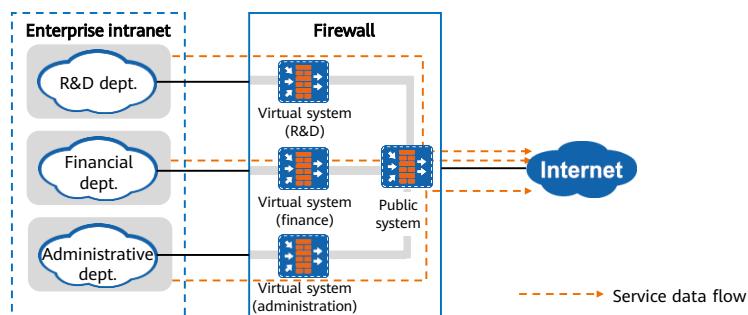
Security Threats to Boundary - Defense Against Network Attacks

- A firewall is typically deployed at the egress of an enterprise intranet. After the attack defense function is enabled, the firewall can distinguish between legitimate traffic and attack traffic, permit legitimate traffic, and block attack traffic. This function ensures that intranet servers and PCs run properly, thereby enabling uninterrupted services for authorized users.



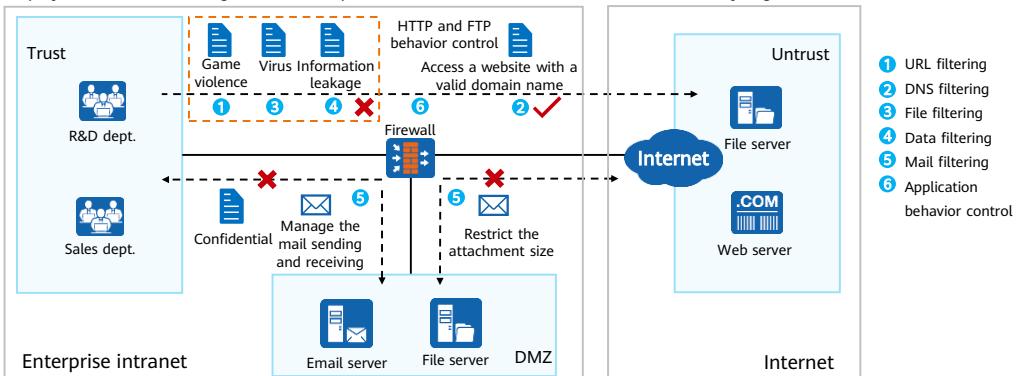
Security Requirements at the Boundary - Network Isolation

- Large- and medium-sized enterprises typically have complex organizational structures and a large number of network devices, facing complex network environments. As the enterprise services expand, each service department has its own security requirements. If all security configurations are made on the same firewall, the firewall configuration will be complicated and the administrator's operations are prone to errors. The firewall virtualization technology allows the administrator to divide a network into multiple subnets and configure a virtual system for each subnet, simplifying service management.



Security Requirements at the Boundary - Application Content Security

- 70% of information security events result from internal employees' improper operations or their lack of security awareness. In terms of compliance and service requirements, enterprises need to manage employee behaviors and application content to ensure that employees do not violate regulations, enterprise secrets are not disclosed, and intranet security is guaranteed.



21 Huawei Confidential

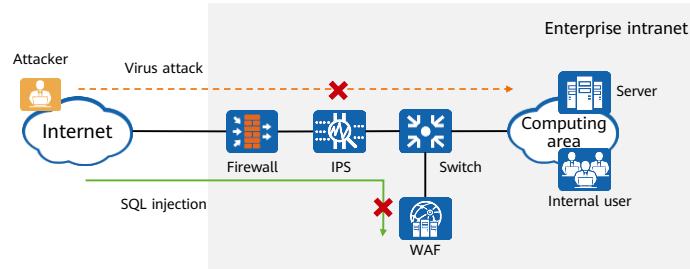
HUAWEI

- Content security filtering:

- URL filtering regulates online behaviors by controlling URLs that users can access, thereby permitting or rejecting users' access to specified web page resources.
- DNS filtering is implemented in the domain name resolution phase to prevent employees from accessing illegal content or malicious websites, which may cause threats such as viruses, Trojan horses, and worms.
- File blocking blocks the transmission of certain types of files, which reduces risks of executing malicious codes and infecting viruses on the internal network and prevents employees from transmitting enterprises' confidential files to the Internet.
- Data filtering falls into two types: file data filtering and application data filtering. File data filtering filters the uploaded and downloaded files by keyword. The administrator can specify the file transfer protocols or the types of files to be filtered. Application data filtering filters application content by keyword. The device filters different data for different applications.
- Mail filtering: filters mails by checking the email addresses of the sender and recipient, attachment size, and number of attachments.
- The application behavior control function is used to accurately regulate users' HTTP and FTP behaviors (such as upload and download).

Security Threats in the Computing Environment - Application Threats

- The internal network computing area involves hardware devices such as office computers, servers, and mobile endpoints, as well as the systems, applications, and data on the devices. When vulnerabilities occur on the intranet, the intranet is prone to various application threats, such as viruses and intrusions. Security implementation engineers usually deploy security devices to protect the computing area. Security O&M engineers detect vulnerabilities promptly through vulnerability scan in daily work, install patches, and sometimes perform penetration testing to prevent potential threats to the network.



Security Requirements in the Management Center - Emergency Response

- Security O&M engineers need to learn about the network security posture to identify security risks and prevent or respond to security threats promptly.
- Emergency response refers to the preparations made by an organization to respond to emergencies and major information security incidents. It also includes the measures taken after the incidents occur.
- Emergency response can reduce the loss suffered by enterprises and the negative impact caused by information security incidents.

Security events

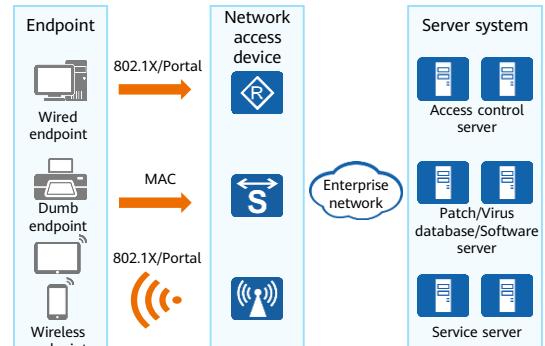
A security incident affects the proper running of a system. Security incidents include hacker intrusion, information theft, denial of service (DoS) attacks, and abnormal network traffic.

Emergency response

Organizations take preparations to cope with unexpected or major information security incidents and a series of measures after security incidents occur.

Security Requirements in the Management Center - Access Control

- If an employee with excessive permission operates improperly, for example, the employee deletes the database by mistake, the security risks of the service system increase.
- Moreover, if visitors in an enterprise access the enterprise's intranet without authorization, the service system may be damaged and key information assets may be leaked.
- In this case, access users need to be authenticated and authorization for them needs to be managed. As such, access control is necessary for every campus network.



Access control example

Quiz

1. (Multiple-Answer Question) Which of the following items are not included in infrastructure security? ()
 - A. Encrypted transmission
 - B. Vulnerability scan
 - C. Situational awareness
 - D. Network reliability
2. (True or false) Firewall reliability is a security measure for the boundary. ()
 - A. T
 - B. F

1. BC

2. B

Summary

- This course provides the classification and responsibilities of cyber security engineers, the capability models for security implementation engineers and security O&M engineers, and the coverage of the Huawei HCIP-Security certification course based on the capability models.
- After learning this course, you will be able to describe the classification of security engineers and talent requirements for related positions, and learn about the HCIP-Security course outline.

Recommendations

- Huawei official websites:
 - Enterprise service: <https://e.huawei.com/en/>
 - Technical support: <https://support.huawei.com/enterprise/en/index.html>
 - Online learning: <http://learning.huawei.com/en/>

Acronyms and Abbreviations (1/2)

Acronym/Abbreviation	Full Name
5G	5th Generation
AntiDDoS	Anti Distributed Denial of Service
DNS	Domain Name Server
DDoS	Distributed Denial of Service
ERP	Enterprise Resource Planning
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISP	Internet Service Provider
IPsec	Internet Protocol Security
SNMP	Simple Network Management Protocol

Acronyms and Abbreviations (2/2)

Acronym/Abbreviation	Full Name
SQL	Structured Query Language
SSL	Universal Serial Bus
TCP/IP	Transmission Control Protocol/Internet Protocol
URL	Uniform Resource Locator
WAF	Web Application Firewall
XSS	Cross-Site Scripting

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。
Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

Copyright©2022 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product performance, market position, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.



Firewall High Reliability Technologies



Foreword

- Firewalls, as key network elements (NEs), are usually deployed at the border of an enterprise's network or between different areas of an enterprise's intranet. To ensure stable and reliable running of an enterprise's network, multiple technologies are required to improve the reliability of the deployed firewalls.
- Firewall high reliability technologies are typically implemented through device redundancy and link redundancy. This course describes the principles and application scenarios of firewall high reliability technologies.

Objectives

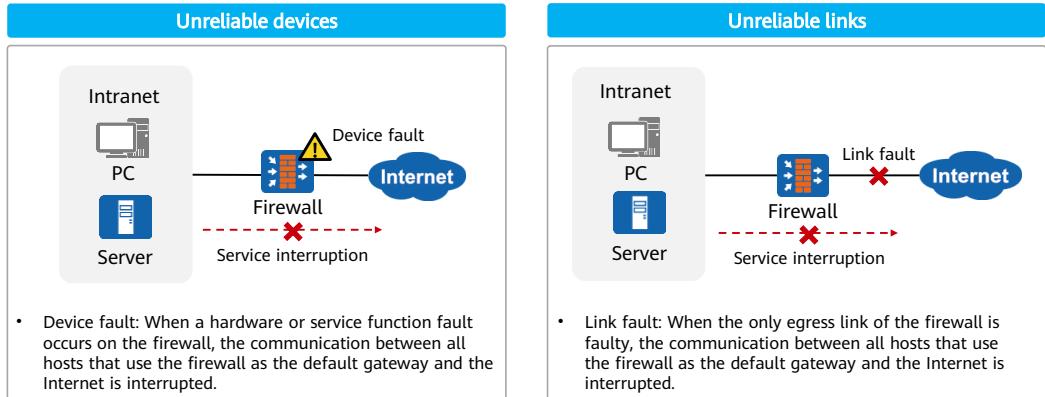
- Upon completion of this course, you will be able to:
 - Describe the principles of firewall high reliability technologies.
 - Understand the high reliability networking mode of the firewall.
 - Describe the application scenarios of firewall high reliability technologies.
 - Configure firewall high reliability technologies.

Contents

- 1. Overview of Firewall High Reliability Technologies**
2. Firewall Hot Standby
3. Firewall Link High Reliability
4. Hot Standby Version Upgrade and Troubleshooting

Background of Firewall High Reliability Technologies

- Unreliable hardware in the network architecture is mainly caused by unreliable devices and links. The following uses the firewall as an example:



Overview of Firewall High Reliability Technologies

- Firewall high reliability is classified into device high reliability and link high reliability.

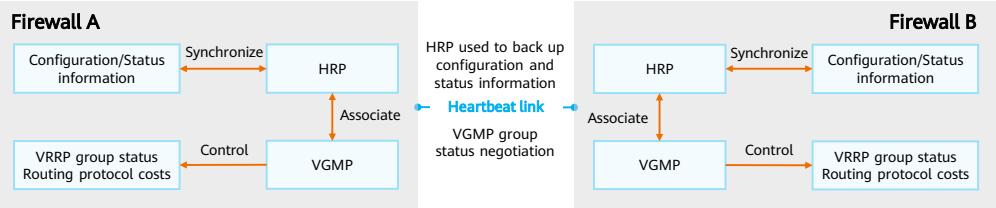
Device high reliability technologies				
Hot standby	Cross-DC cluster	Hardware bypass		
Two firewalls work in hot standby mode. When one firewall is faulty, the other firewall takes over services to ensure service continuity.	The firewalls in other data centers can take over services from the faulty firewall in a data center. In this way, firewalls in different data centers back up each other.	The hardware bypass function enables a faulty firewall to directly forward traffic without processing it, thereby preventing service interruption.		
Link high reliability technologies				
Eth-Trunk	IP-Link	BFD	Link-Group	Health check
Multiple physical interfaces are bound as a logical interface to improve link reliability.	ARP or ICMP packets are periodically sent to check link availability.	BFD control packets are periodically sent to check the availability of links between devices or systems.	Different interfaces are added to a logical group, known as a link-group, which ensures the status consistency of these interfaces.	The health check function detects service availability, link availability, or link latency. Currently, this function is used together with the intelligent uplink selection feature of the firewall.

Contents

1. Overview of Firewall High Reliability Technologies
2. **Firewall Hot Standby**
 - Hot Standby Overview
 - VRRP-based Hot Standby
 - Routing Protocol-based Hot Standby
 - Hot Standby in Transparent Mode
3. Firewall Link High Reliability
4. Hot Standby Version Upgrade and Troubleshooting

Hot Standby Working Mechanism

- Huawei Redundancy Protocol (HRP) is used to back up key configuration commands and status information between the active and standby firewalls. Status information includes the session table, server mapping table, blacklist and whitelist, and NAT mapping table.
- VRRP Group Management Protocol (VGMP) manages Virtual Router Redundancy Protocol (VRRP) groups in a unified manner and ensures the status consistency of multiple VRRP groups. The VGMP status also affects the costs of routing protocols.
- Backup channel: It is also called the heartbeat link and is used for HRP and VGMP communication.



7 Huawei Confidential

 HUAWEI

- **VGMP status:** When the VGMP group status of a firewall is active, it ensures that all VRRP groups in the VGMP group are in active state. In this way, all packets pass through the firewall and the firewall becomes the active firewall. In this case, the VGMP group status of the other firewall is standby, and this firewall becomes the standby firewall.

Hot Standby Working Modes

- The firewalls in a hot standby group support active/standby and load sharing modes.

Active/standby mode	Load sharing mode
<ul style="list-style-type: none">There are two devices — an active and a standby one. Normally, the active device processes service traffic. If this device fails, the standby device takes over to ensure service continuity.A single device processes traffic, making route planning and fault locating simpler compared to the load sharing mode.In active/standby mode, the standby device does not carry any service traffic, resulting in low resource usage.	<ul style="list-style-type: none">The two devices back up each other. During normal operation, both devices share the entire network's service traffic. If one device fails, the other device takes over all services to ensure service continuity.The networking scheme and configuration are more complex compared to the active/standby mode.In load sharing mode, traffic is processed by two devices, which improves the overall service throughput of the firewall.Only half of the services need to be switched if a device in load sharing mode fails, making the switchover faster than in active/standby mode.

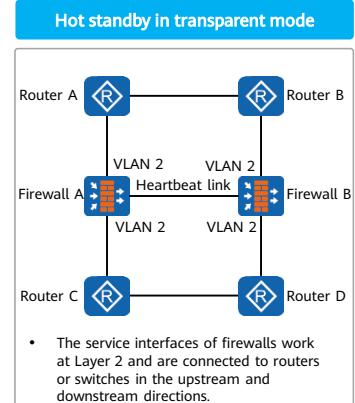
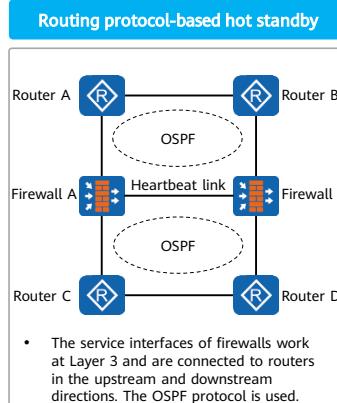
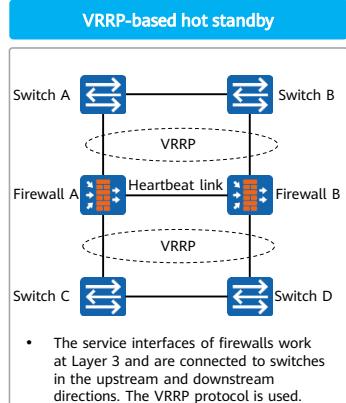
8 Huawei Confidential



- Precautions for backup in different modes:
 - In active/standby mode, configuration commands and status information are backed up from the active device to the standby device.
 - In load sharing mode, both firewalls are active. Therefore, if both firewalls are allowed to back up commands to each other, command overwrite or conflict problems may occur. To centrally manage the configurations of the two firewalls, you need to configure the designated active and standby devices.
 - In load sharing mode, the sender of the configuration backup command is the designated active device (identified by HRP_M), and the receiver is the designated standby device (identified by HRP_S). Configuration commands can be backed up only from the designated active device to the designated standby device. Status information, however, can be mutually backed up.

Introduction to Hot Standby Scenarios

- Based on the firewall networking mode, hot standby can be classified into the following scenarios, each of which supports both the active/standby mode and load sharing mode.

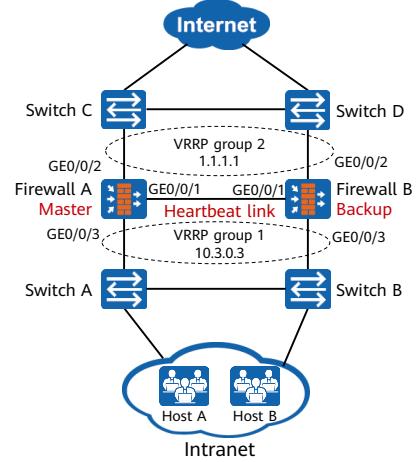


Contents

1. Overview of Firewall High Reliability Technologies
2. **Firewall Hot Standby**
 - Hot Standby Overview
 - **VRRP-based Hot Standby**
 - Routing Protocol-based Hot Standby
 - Hot Standby in Transparent Mode
3. Firewall Link High Reliability
4. Hot Standby Version Upgrade and Troubleshooting

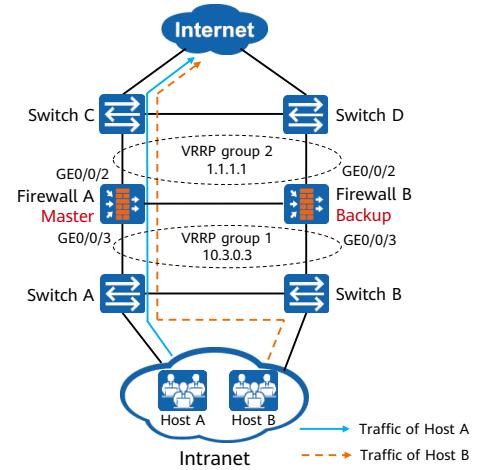
Application Scenario of the Active/Standby Mode

- Networking description:
 - As shown in the figure, two firewalls are deployed at the egress of the enterprise network to implement hot standby in scenarios requiring high reliability.
- Networking analysis:
 - VGMP group status of firewalls: Firewall A is the active firewall, and its VGMP group status is active. Firewall B is the standby firewall, and its VGMP group status is standby.
 - VRRP group: Add the downlink interfaces of the firewalls to VRRP group 1 and the uplink interfaces of the firewalls to VRRP group 2. The status of VRRP groups 1 and 2 on Firewall A is set to master, and VRRP groups on Firewall B is set to backup.
 - Backup interface: GE0/0/1 interfaces on firewalls A and B are heartbeat interfaces, and the heartbeat link connecting them is used as the backup link.



Traffic Forwarding Process in Active/Standby Mode

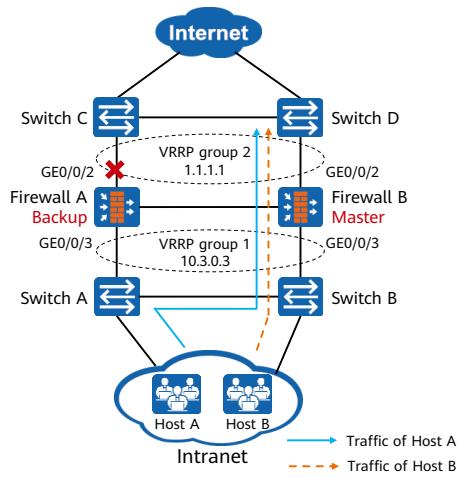
- Traffic forwarding process:
 - Firewall A sends gratuitous ARP packets to Switch A and Switch C to update the MAC address tables of the switches.
 - When Host A accesses the Internet, it queries the gateway MAC address (MAC address of the VRRP virtual IP address) through ARP. Firewall A replies with the VRRP virtual MAC address. Host A then sends service packets to Switch A, which forwards the traffic to Firewall A based on the MAC address table. Firewall A then forwards the traffic to the Internet.
 - The process of forwarding returned traffic is similar and is not described here.



- Configuration and status backup: The configuration and status of Firewall A are backed up to Firewall B through the heartbeat link in real time.

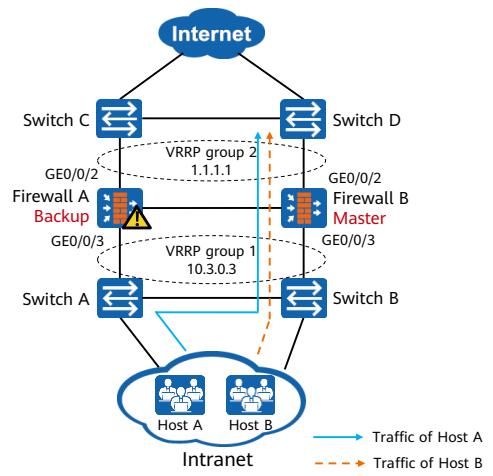
Firewall Active/Standy Switchover (1/2)

- The active/standby switchover is triggered when the service interface or service link of a firewall is faulty.
 - As shown in the figure, when GE0/0/2 of Firewall A is faulty, the priority of Firewall A in the VGMP group decreases and Firewall A sends a VGMP request packet.
 - After receiving the VGMP request packet, Firewall B compares the VGMP group priority in the packet with its own VGMP group priority and sends a VGMP response packet.
 - After receiving the response packet, Firewall A switches its VGMP group status to standby, and the status of VRRP groups 1 and 2 to backup.
 - Firewall B switches its VGMP group status to active, and the status of VRRP groups 1 and 2 to master.
 - Firewall B sends gratuitous ARP packets to Switch B and Switch D to update the MAC address table of the switches. Service traffic is switched to Firewall B.



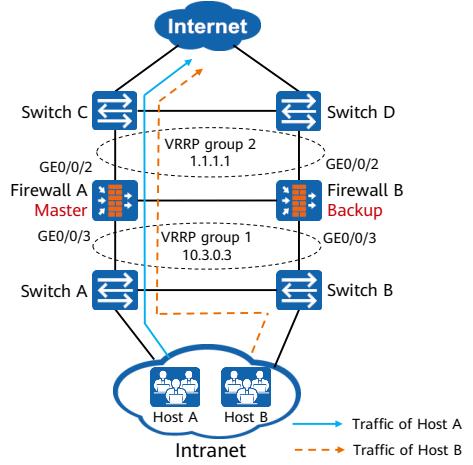
Firewall Active/Standy Switchover (2/2)

- An active/standby switchover is triggered when a firewall is faulty.
 - Firewall A is faulty and does not send HRP Hello packets. Firewall B does not receive HRP Hello packets from Firewall A within five packet transmission intervals and becomes the active device. Firewall B then changes its VGMP group status to active and the status of VRRP groups 1 and 2 on Firewall B switches to master.
 - Firewall B sends gratuitous ARP packets to Switch B and Switch D to update the MAC address table of the switches. Service traffic is switched to Firewall B.



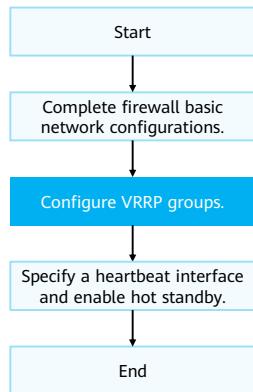
Firewall Active/Standy Switchback

- After a fault is rectified, active/standby switchback is triggered.
 - After Firewall A recovers, its VGMP group priority increases. By default, after 60s, Firewall A sends a VGMP request packet.
 - After receiving the VGMP request packet, Firewall B compares the VGMP group priority in the packet with its own VGMP group priority. If Firewall B finds that its VGMP group priority is the same as or lower than that of Firewall A, Firewall B returns a VGMP response packet and switches its VGMP group status to standby and the status of VRRP groups 1 and 2 to backup.
 - After receiving the response packet, Firewall A switches its VGMP group status to active and the status of VRRP groups 1 and 2 to master.
 - Firewall A sends gratuitous ARP packets to Switch A and Switch C to update the MAC address table of the switches. Service traffic is switched to Firewall A.



Configuration Roadmap of the Active/Standby Mode

- Configuration roadmap:



- Key configurations:

- Add the uplink and downlink service interfaces of Firewall A to VRRP groups and set the VRRP group status to active.

```
[FW_A] interface GE0/0/2  
[FW_A-GE0/0/2] vrrp vrid 1 virtual-ip 1.1.1.1 active  
[FW_A-GE0/0/2] quit  
[FW_A] interface GE0/0/3  
[FW_A-GE0/0/3] vrrp vrid 2 virtual-ip 10.3.0.3 active  
[FW_A-GE0/0/3] quit
```

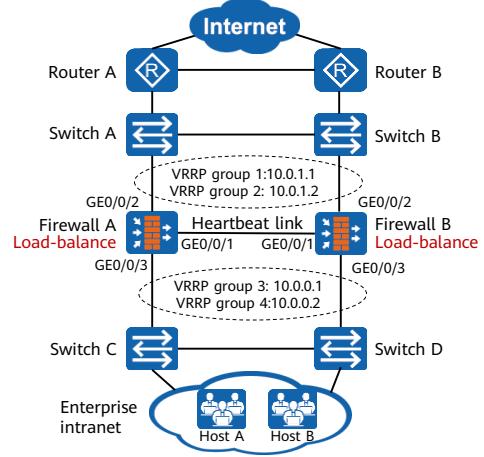
- Add the uplink and downlink service interfaces of Firewall B to VRRP groups and set the VRRP group status to standby.

```
[FW_B] interface GE0/0/2  
[FW_B-GE0/0/2] vrrp vrid 1 virtual-ip 1.1.1.1 standby  
[FW_B-GE0/0/2] quit  
[FW_B] interface GE0/0/3  
[FW_B-GE0/0/3] vrrp vrid 2 virtual-ip 10.3.0.3 standby  
[FW_B-GE0/0/3] quit
```

Application Scenario of the Load Sharing Mode

- Networking description:
 - As shown in the figure, the uplink and downlink service interfaces of the firewalls work at Layer 3. The two firewalls forward traffic for users at the same time and back up each other to improve network reliability.
- Networking analysis:
 - If two firewalls work in load sharing mode, a master VRRP group must exist on each firewall.
 - VRRP groups 1 and 3 on Firewall A are in master state, and VRRP groups 2 and 4 on Firewall A are in backup state.
 - VRRP groups 1 and 3 on Firewall B are in backup state, and VRRP groups 2 and 4 on Firewall B are in master state.
 - The VGMP groups on the two devices are in load-balance state.

17 Huawei Confidential

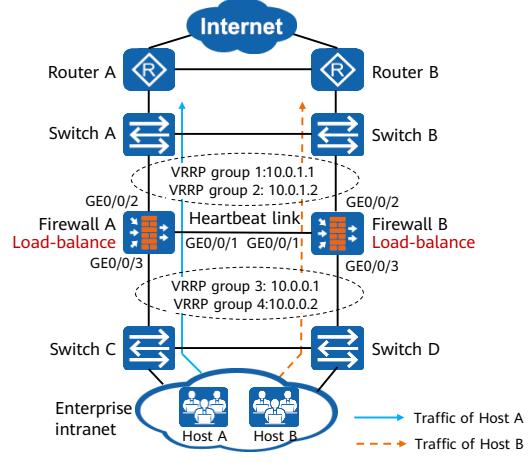


HUAWEI

Traffic Forwarding Process of the Load Sharing Mode

- Traffic forwarding process:
 - The gateway address of some hosts on the intranet is set to the virtual IP address 10.0.0.1 of VRRP group 3. When these hosts access the Internet, they send ARP requests to request the MAC address mapped to 10.0.0.1. VRRP group 3 on Firewall A is in master state, and Firewall A responds to ARP requests from these hosts. VRRP group 3 on Firewall B is in backup state, and Firewall B does not respond to the ARP requests. The MAC address table of the switch and the ARP cache tables of the hosts are updated based on the ARP reply packets from Firewall A to enable the traffic sent from the hosts to the Internet to be diverted to Firewall A for processing.
 - The gateway address of the other hosts is set to the virtual IP address 10.0.0.2 of VRRP group 4. When these hosts access the Internet, they send ARP requests to request the MAC address mapped to 10.0.0.2. In this case, only Firewall B responds to the ARP requests. Therefore, the traffic of these hosts is diverted to Firewall B for forwarding.

18 Huawei Confidential

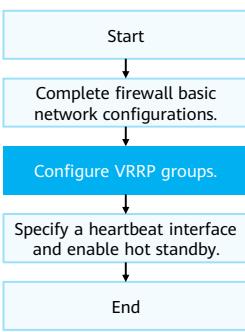


HUAWEI

- Similarly, the next-hop address of the route from Router A to the intranet is set to the virtual IP address 10.0.1.1 of VRRP group 1. The traffic sent from Router A to the intranet is diverted to Firewall A for processing. The next-hop address of the route from Router B to the intranet is set to the virtual IP address 10.0.1.2 of VRRP group 2. The traffic sent from Router B to the intranet is diverted to Firewall B for processing.

Configuration Roadmap of the Load Sharing Mode

- Configuration roadmap:



- Key configurations:

- Configure two VRRP groups on each firewall.

- [FW_A] interface GigabitEthernet 0/0/2
[FW_A-GEO/0/2] vrrp vrid 1 virtual-ip 10.0.1.1 active
[FW_A-GEO/0/2] vrrp vrid 2 virtual-ip 10.0.1.2 standby
[FW_A] interface GigabitEthernet 0/0/3
[FW_A-GEO/0/3] vrrp vrid 3 virtual-ip 10.0.0.1 active
[FW_A-GEO/0/3] vrrp vrid 4 virtual-ip 10.0.0.2 standby

- [FW_B] interface GigabitEthernet 0/0/2
[FW_B-GEO/0/2] vrrp vrid 1 virtual-ip 10.0.1.1 standby
[FW_B-GEO/0/2] vrrp vrid 2 virtual-ip 10.0.1.2 active
[FW_B] interface GigabitEthernet 0/0/3
[FW_B-GEO/0/3] vrrp vrid 3 virtual-ip 10.0.0.1 standby
[FW_B-GEO/0/3] vrrp vrid 4 virtual-ip 10.0.0.2 active

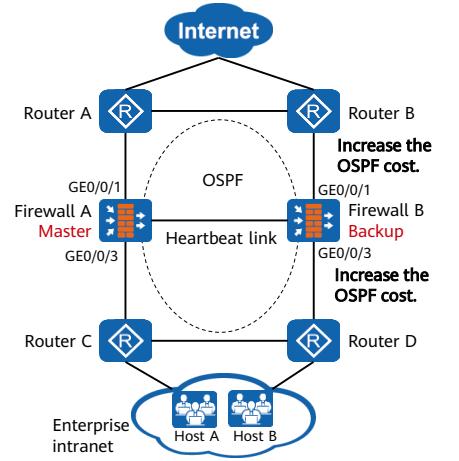
Contents

1. Overview of Firewall High Reliability Technologies
2. **Firewall Hot Standby**
 - Hot Standby Overview
 - VRRP-based Hot Standby
 - Routing Protocol-based Hot Standby
 - Hot Standby in Transparent Mode
3. Firewall Link High Reliability
4. Hot Standby Version Upgrade and Troubleshooting

Application Scenario of the Active/Standby Mode

- Networking description:
 - As shown in the figure, the uplink and downlink service interfaces of the firewalls work at Layer 3 and are directly connected to routers. OSPF runs between the firewalls and routers.
- Networking analysis:
 - Firewall A is the active firewall, and its VGMP group status is active. Firewall B is the standby firewall, and its VGMP group status is standby.
 - After hot standby is enabled, the firewall can dynamically adjust the OSPF path cost based on the VGMP group status. The VGMP group of the active firewall is in active state, and the firewall advertises routes according to the OSPF route configuration without changing the cost. The VGMP group of the standby firewall is in standby state, and the standby firewall increases its OSPF route cost to make the route a standby route.

21 Huawei Confidential

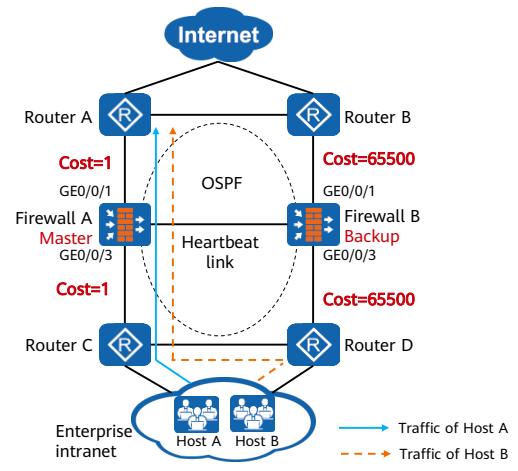


HUAWEI

- The firewalls are connected to Layer 3 devices in the upstream and downstream directions. In this scenario, VRRP groups cannot be configured, therefore active and standby devices cannot be determined through VRRP, and the status of service interfaces directly connected to firewalls cannot be monitored through VRRP.
- The **hrp adjust enable** command is used to enable the route cost adjustment function. After this command is run, a firewall dynamically adjusts the costs of routing protocols such as OSPF based on the active/standby status.

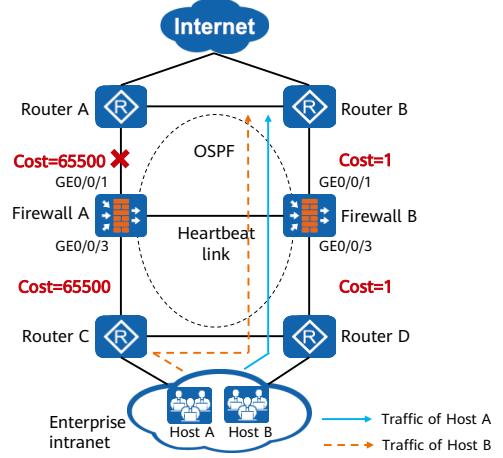
Traffic Forwarding Process in Active/Standby Mode

- Traffic forwarding process:
 - In normal cases, Firewall A advertises routes according to the OSPF configuration, and the cost of the OSPF routes advertised by Firewall B is changed to 65500. The cost of Firewall A's link is far smaller than that of Firewall B's link. When forwarding traffic, a router selects a path with a smaller cost. Therefore, traffic between the intranet and Internet is diverted to Firewall A for forwarding.
 - In the figure, the interface bandwidth of Firewall A is 1000 Mbit/s. Therefore, its OSPF cost is 1.



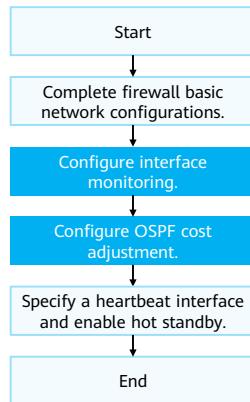
Firewall Active/Standy Switchover

- Active/Standy switchover process:
 - When the uplink service interface of Firewall A is faulty, the status of the VGMP group on Firewall A changes to standby, and the status of the VGMP group on Firewall B changes to active.
 - Firewalls A and B adjust the OSPF costs based on the VGMP group status.
 - The cost of the OSPF route advertised by Firewall A changes to 65500.
 - The cost of the OSPF route advertised by Firewall B changes to 1.
 - After OSPF route convergence is complete, traffic between the intranet and Internet is diverted to Firewall B for forwarding.



Configuration Roadmap of the Active/Standby Mode

- Configuration roadmap:



- Key configurations:

- Run the **hrp track interface** command on Firewall A and Firewall B to monitor uplink and downlink service interfaces.

```
[FW_A] hrp track interface GE0/0/1  
[FW_A] hrp track interface GE0/0/3  
[FW_B] hrp track interface GE0/0/1  
[FW_B] hrp track interface GE0/0/3
```

- Configure the cost adjustment commands on Firewall A and Firewall B.

```
[FW_A] hrp adjust ospf-cost enable  
[FW_B] hrp adjust ospf-cost enable
```

Note: If a firewall is the active device, it directly advertises the learned OSPF routes. If a firewall is the standby device, it advertises OSPF routes with the cost of 65500.



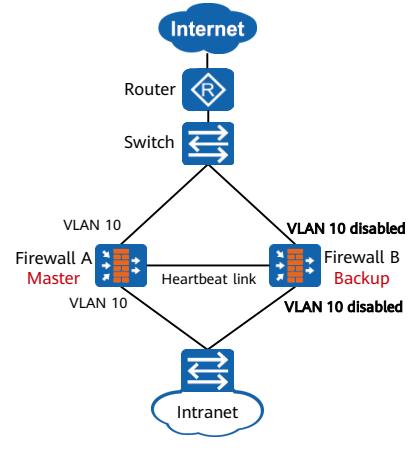
Contents

1. Overview of Firewall High Reliability Technologies
2. **Firewall Hot Standby**
 - Hot Standby Overview
 - VRRP-based Hot Standby
 - Routing Protocol-based Hot Standby
 - **Hot Standby in Transparent Mode**
3. Firewall Link High Reliability
4. Hot Standby Version Upgrade and Troubleshooting

Application Scenario of the Active/Standby Mode

- Networking description:
 - As shown in the figure, the uplink and downlink service interfaces of the firewalls work at Layer 2 and are directly connected to Layer 2 switches. The uplink and downlink service interfaces of the firewalls are added to the same VLAN. The firewalls must be able to monitor the availability of service interfaces.
- Networking analysis:
 - Firewall A is the active firewall, and its VGMP group status is active. Firewall B is the standby firewall, and its VGMP group status is standby.
 - After hot standby is enabled, the firewalls can enable or disable the VLAN based on the VGMP group status (VLAN monitoring needs to be configured).
 - When the VGMP group is in active state, the firewall enables the VLAN monitored by the VGMP group so that packets with this VLAN ID can be forwarded.
 - When the VGMP group is in standby state, the firewall disables the VLAN monitored by the VGMP group so that packets with this VLAN ID cannot be forwarded.

26 Huawei Confidential

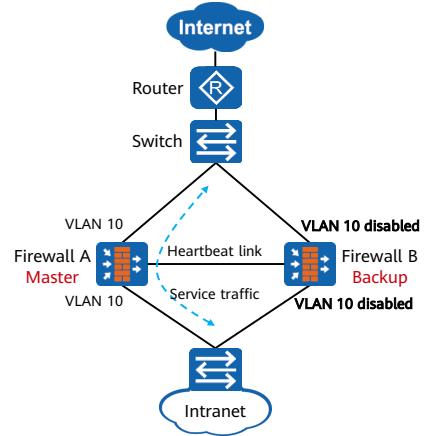


 HUAWEI

- On this network, the firewalls are transparently connected to the original switch network without changing the network topology.

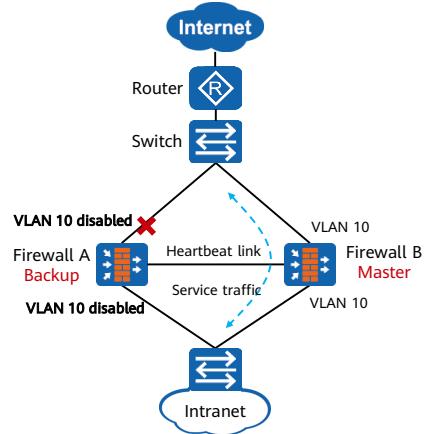
Traffic Forwarding Process in Active/Standby Mode

- Traffic forwarding process:
 - When both firewalls work normally, VLAN 10 is disabled on Firewall B because Firewall B is the standby firewall. VLAN 10 on Firewall A is enabled. The upstream and downstream switches can learn MAC addresses only from the interfaces connected to Firewall A, and traffic is diverted to Firewall A for processing.



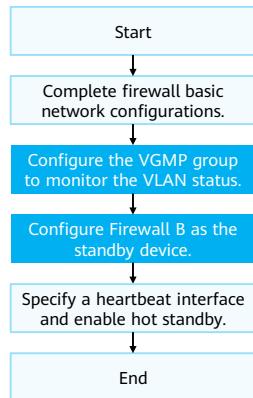
Firewall Active/Standy Switchover

- Switchover process:
 - When the uplink service interface of Firewall A is faulty, the status of the VGMP group on Firewall A changes to standby, and the status of the VGMP group on Firewall B changes to active.
 - Firewalls A and B adjust the VLAN status based on the VGMP group status: VLAN 10 on Firewall A is disabled, and VLAN 10 on Firewall B is enabled.
 - At the same time, all interfaces added to VLAN 10 on Firewall A go Down, triggering the upstream and downstream switches to delete the MAC address table.
 - When packets reach the upstream and downstream switches, the packets are flooded in VLAN 10 because no MAC address is matched. Then, the switches learn the MAC address table from the interface connected to Firewall B, and subsequent traffic is diverted to Firewall B for processing.



Configuration Roadmap of the Active/Standby Mode

- Configuration roadmap:



- Key configurations:

- Configure VGMP groups on Firewall A and B to monitor the status of the VLANs corresponding to the uplink and downlink service interfaces.

- [FW_A] hrp track vlan 10
[FW_B] hrp track vlan 10

- Configure Firewall B as the standby device.

- [FW_B] hrp standby-device

- Configure the VGMP group to monitor the VLAN status.

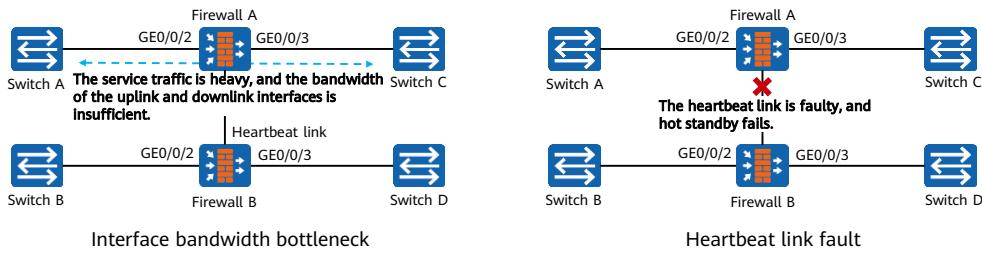
- Application scenario: When a firewall works at Layer 2, to enable the VGMP group to monitor the status of Layer 2 service interfaces, add uplink and downlink service interfaces to the same VLAN and configure **hrp track vlan**.
 - Function: After **hrp track vlan** is configured, each faulty interface in the VLAN decreases the priority of the VGMP group by 2. After **hrp track vlan** is configured on the standby device, packets with this VLAN ID cannot be forwarded.
 - Command: **hrp track vlan *vlan-id***.

Contents

1. Overview of Firewall High Reliability Technologies
2. Firewall Hot Standby
- 3. Firewall Link High Reliability**
 - Eth-Trunk
 - IP-Link
 - BFD
 - Link-Group
4. Hot Standby Version Upgrade and Troubleshooting

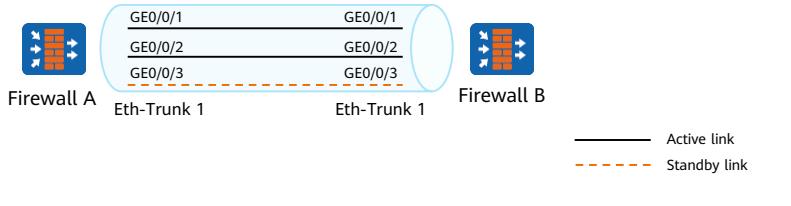
Technical Background of Eth-Trunk

- Firewalls are key network devices on enterprise networks. Although hot standby can significantly improve device reliability, the following problems may still exist from the perspective of the overall network:
 - If hot standby switchover occurs frequently, the network is unstable.
 - In scenarios with heavy service traffic, the link bandwidth may have a bottleneck and cannot meet service requirements (especially processing requirements of burst service traffic).
 - If a heartbeat link is faulty, HRP/VGMP communication will fail and hot standby will be ineffective, interrupting services.



Introduction to Eth-Trunk

- Eth-Trunk, also called link aggregation, bundles multiple physical Ethernet links into a logical link to increase bandwidth and improve link reliability.
- Eth-Trunk provides the following functions:
 - Increased bandwidth: The maximum bandwidth of an Eth-Trunk interface is the sum of bandwidth of its member interfaces.
 - Traffic load balancing: Traffic load can be balanced in a link aggregation group (LAG).
 - Higher reliability: When an active link fails, traffic can be switched to other available member links, improving reliability of the Eth-Trunk interface.



32 Huawei Confidential

HUAWEI

- LAG and Eth-Trunk interface:
 - A LAG is a logical link formed by binding several Ethernet links.
 - Each LAG corresponds to a unique logical interface, known as a LAG interface or an Eth-Trunk interface.
- Active and inactive interfaces: There are two types of member interfaces in a LAG: active and inactive. An interface that forwards data is active, while an interface that does not forward data is inactive.
- Active and inactive links: The link connected to an active interface is an active link, and that connected to an inactive interface is an inactive link.
- Link aggregation modes for Eth-Trunk:
 - Manual mode: An Eth-Trunk interface is manually created and member interfaces are manually added to the Eth-Trunk interface. In manual mode, all links are active. If a link is disconnected, other active links automatically balance traffic.
 - LACP mode: An Eth-Trunk interface is manually created and member interfaces are manually added to the Eth-Trunk interface. In LACP mode, link status negotiation is controlled by the Link Aggregation Control Protocol (LACP), and the link status can be dynamically monitored. This mode is recommended. For details about LACP, see related Huawei product documentation.

Eth-Trunk Configuration Commands

- Create a LAG.

```
[FW] interface eth-trunk trunk-id
```

- Add the Ethernet physical interfaces to the LAG (Ethernet interface view).

```
[FW] interface GigabitEthernet 0/0/1  
[FW-GigabitEthernet0/0/1] eth-trunk trunk-id  
[FW] interface GigabitEthernet 0/0/2  
[FW-GigabitEthernet0/0/2] eth-trunk trunk-id
```

- Configure an IP address for the Eth-Trunk interface.

```
[FW-Eth-Trunk trunk-id] ip address x.x.x.x
```

Checking the Status of the Eth-Trunk Interface

- Check the configuration and status of the Eth-Trunk interface.

```
<FW> display eth-trunk
Eth-Trunk1's state information is:
WorkingMode: NORMAL      Hash arithmetic: According to flow
Least Active-linknumber: 2  Max Bandwidth-affected-linknumber: 8      Operate status: up
Number Of Up Port In Trunk: 2
-----
PortName Status weight
GigabitEthernet0/0/1 Up 1
GigabitEthernet0/0/2 Up 1
```

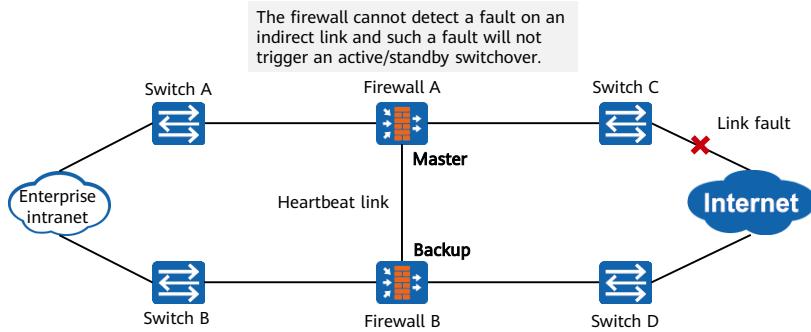
- **WorkingMode** indicates the working mode of an Eth-Trunk interface. The working modes are as follows:
 - NORMAL: manual load balancing mode.
 - STATIC: static LACP mode.
 - BACKUP: manual 1:1 master/backup mode.
- **Hash arithmetic** indicates the load balancing mode of an Eth-Trunk interface. The modes are as follows:
 - According to flow: indicates that load balancing is performed on an Eth-Trunk interface based on flows.
 - According to packet all: indicates that load balancing is performed on an Eth-Trunk interface based on all packets.
- **Least Active-linknumber** indicates the minimum number of active Eth-Trunk member links. If the number of Eth-Trunk member interfaces in Up state is less than the lower limit, the Eth-Trunk interface goes Down.
- **Max Bandwidth-affected-linknumber** indicates the maximum number of links that affect the effective bandwidth of the Layer 2 Eth-Trunk interface.
- **Operate status** indicates the status of the Eth-Trunk interface.
 - Up indicates that the Eth-Trunk interface is in Up state and can forward traffic.
 - Down indicates that the Eth-Trunk interface is in the Down state and cannot forward traffic.
- **Number Of Up Port In Trunk** indicates the number of Up member interfaces in an Eth-Trunk interface.

Contents

1. Overview of Firewall High Reliability Technologies
2. Firewall Hot Standby
- 3. Firewall Link High Reliability**
 - Eth-Trunk
 - IP-Link
 - BFD
 - Link-Group
4. Hot Standby Version Upgrade and Troubleshooting

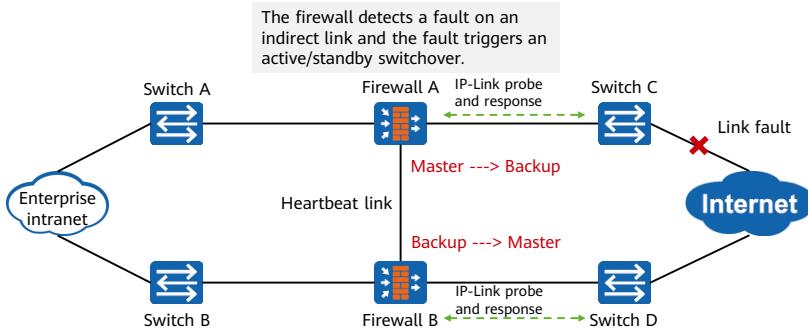
Disadvantages of Traditional Hot Standby

- In traditional hot standby, only the directly connected interface of the firewall is monitored. When the status of the directly connected interface of the active firewall changes from Up to Down, the active/standby switchover is triggered. However, the firewall cannot detect a fault on an indirect link. Such a fault will not trigger an active/standby switchover, and will not interrupt services.



IP-Link Technology

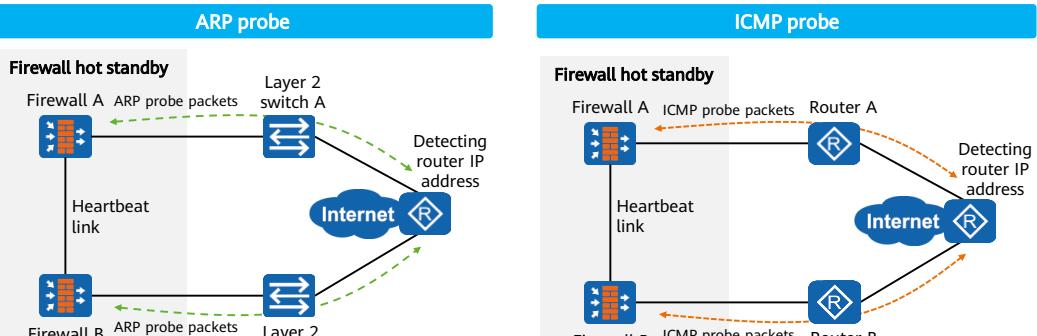
- IP-Link enables the firewall to regularly send probe packets to a specific destination IP address and determines whether faults occur based on the reply packets. IP-Link can detect faults on indirect links. It is used together with hot standby to improve network reliability.



- If the firewall does not receive any response packet within three probe intervals (15s by default) after sending three probe packets, the firewall considers the current link to be faulty, and the IP-Link status changes to Down.
- After the link recovers from the fault, the firewall considers that the link fault is cleared only after it receives three consecutive response packets. Then the IP-Link status changes to Up. That is, the IP-Link status does not immediately become Up after the link fault is rectified. Instead, it becomes Up after three probe intervals (15s by default).

IP-Link Probe Mode

- Based on different probe packets, IP-Link has two probe modes:



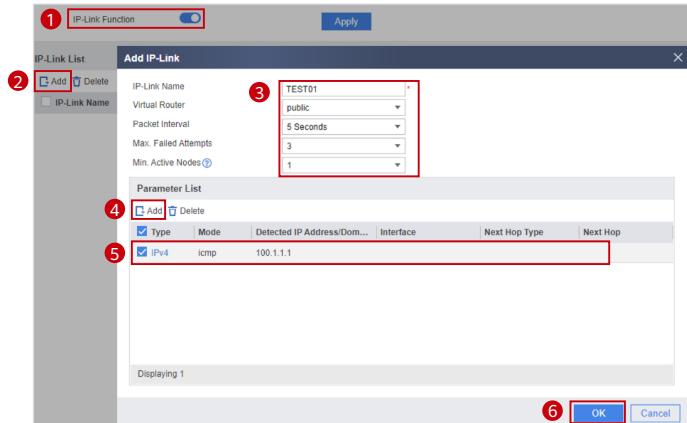
The ARP probe mode can only detect the connectivity of a Layer 2 network.

The ICMP probe mode can detect the connectivity of a Layer 2 or Layer 3 network.

IP-Link Configuration — Web (1/2)

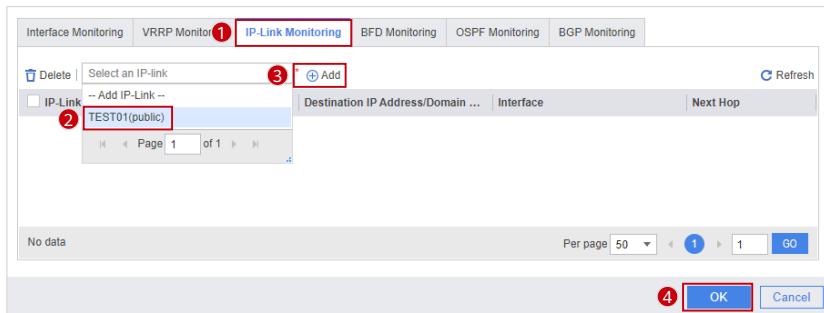
- Log in to the firewall through the web UI, choose **System > High Availability > IP-Link**, and perform the following operations in sequence:

- Enable the IP-Link function.
- Create an IP-link.
- Set the name and parameters of the IP-link.
- Create a member link.
- Set probe parameters for the link.
- Click **OK**.



IP-Link Configuration — Web (2/2)

- Apply the configured IP-link in hot standby.
 - Choose **System > High Availability > Dual-System Hot Standby**, click **Edit** and perform the following operations in sequence:



IP-Link Configuration — CLI

- Configure an IP-link.

```
[FW] ip-link check enable  
[FW] ip-link name test  
[FW-iplink-test] destination 100.1.1.1 interface GigabitEthernet 0/0/3
```

- Apply the configured IP-link in hot standby. When a network fault occurs, the IP-link status becomes Down and the priority of the VGMP group decreases by 2.

```
[FW] hrp track ip-link test
```

- Displays IP-link information.

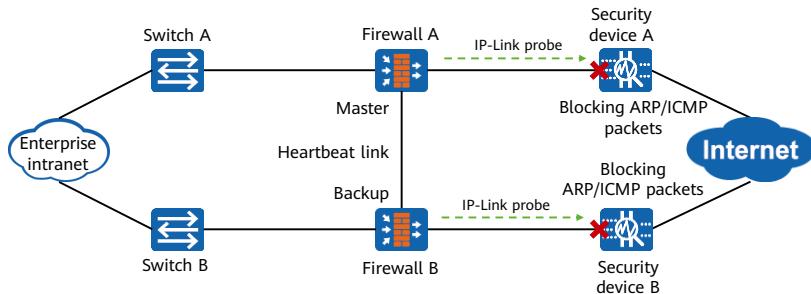
```
[FW] display ip-link  
Current Total Ip-link Number :1  
Name Member State Up/Down/Init  
test 1 up 1 0 0
```

Contents

1. Overview of Firewall High Reliability Technologies
2. Firewall Hot Standby
- 3. Firewall Link High Reliability**
 - Eth-Trunk
 - IP-Link
 - **BFD**
 - Link-Group
4. Hot Standby Version Upgrade and Troubleshooting

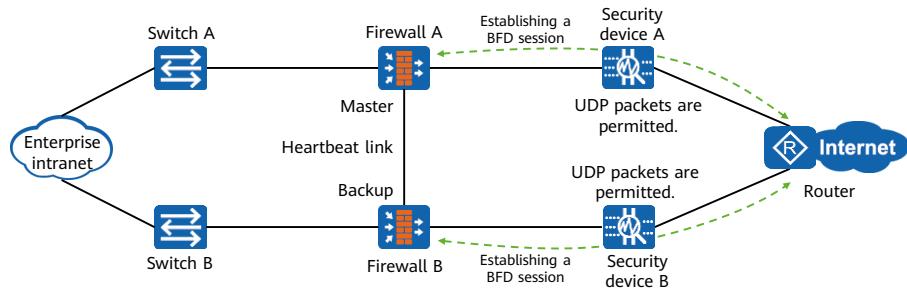
Disadvantages of IP-Link

- IP-Link probe is based on ARP or ICMP. If some security devices on the probe path filter ARP/ICMP packets, IP-Link probe fails.



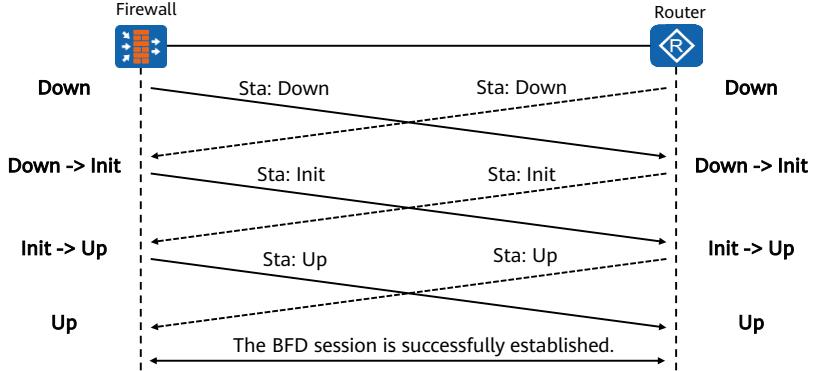
Introduction to BFD

- The Bidirectional Forwarding Detection (BFD) technology is used to rapidly detect communication faults between devices and reports faults to upper protocols.
- BFD performs probing based on UDP packets, whose destination port number is 3784.
- BFD requires that a BFD session be established between the firewall and the device to be detected (such as a router). The devices at both ends of the session must support BFD.



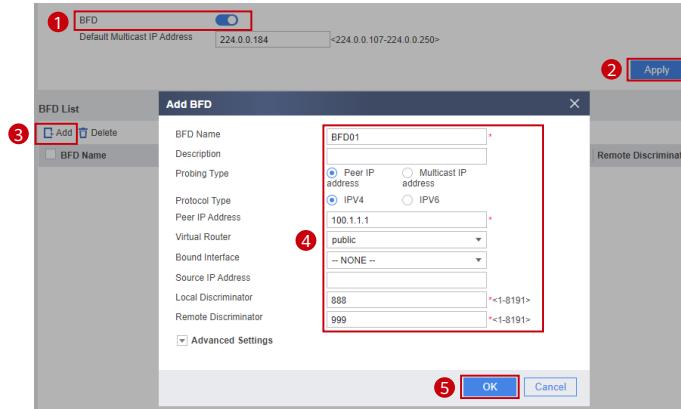
BFD Session Establishment

- BFD distinguishes sessions based on the local and remote discriminators in control packets.
- A BFD session has four states: Down, Init, Up, and AdminDown. The process of establishing a BFD session is as follows:



BFD Configuration — Web UI

- Log in to the firewall through the web UI, choose **System > High Availability > BFD**, and perform the following operations in sequence:



46 Huawei Confidential

 HUAWEI

BFD Configuration — CLI

- Enable BFD globally and enter the global BFD view.

```
[FW] bfd
```

- Create a static BFD session by specifying the peer IP address.

```
[FW] bfd cfg-name bind peer-ip peer-ip [ vpn-instance vpn-instance-name ] [ interface interface-type interface-number [ nexthop { nexthop-address | dhcp } ] ] [ source-ip source-ip ]
```

This command is applicable to a Layer 3 interface that has an IP address.

- Configure discriminators.

```
[FW-bfd-session-name] discriminator local local-dscr-value
```

Configure a local discriminator.

```
[FW-bfd-session-name] discriminator remote remote-dscr-value
```

Configure a remote discriminator.

- Commit the configuration.

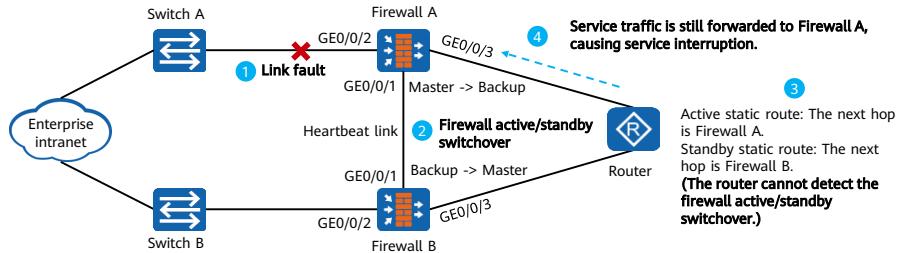
```
[FW-bfd-session-name] commit
```

Contents

1. Overview of Firewall High Reliability Technologies
2. Firewall Hot Standby
- 3. Firewall Link High Reliability**
 - Eth-Trunk
 - IP-Link
 - BFD
 - Link-Group**
4. Hot Standby Version Upgrade and Troubleshooting

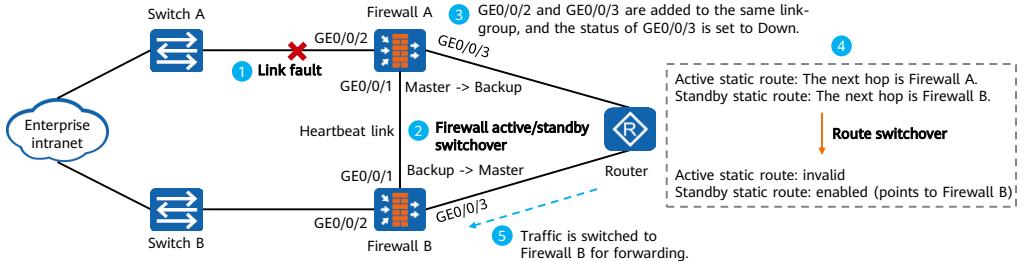
Problems of Hot Standby in Static Routing Scenarios

- In the following scenario, Firewall A is the active firewall, and Firewall B is the standby firewall. Both firewalls are directly connected to the router. Two static routes are configured on the router for accessing the enterprise intranet. The active static route points to Firewall A, and the standby static route points to Firewall B. Data traffic is forwarded by Firewall A.
- When the link of GE0/0/2 on Firewall A is faulty, an active/standby switchover is triggered, and Firewall B becomes the active firewall. However, the router cannot detect the switchover and still forwards service traffic to Firewall A, causing service interruptions.



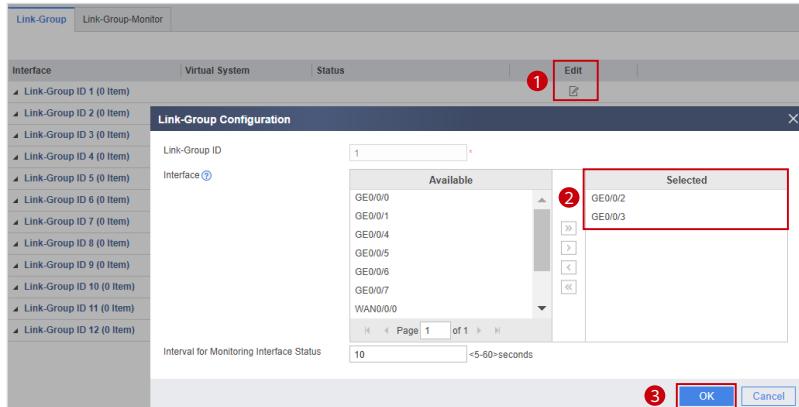
Link-Group Principles

- The Link-Group function can group multiple interfaces of a firewall into a logical group. The interfaces in the logical group remain in the same state (Up/Down).
 - If any interface in a link-group fails, the system changes the status of all other interfaces to Down.
 - The system sets the status of the interfaces in the group to Up only after all interfaces recover.
- Configure the Link-Group function so that the network devices directly connected to the firewall can detect the active/standby switchover and switch routes to restore services.



Link-Group Configuration — Web UI

- Log in to the firewall through the web UI, choose **System > High Availability > Link-Group**, and perform the following operations in sequence:



Link-Group Configuration — CLI

- Add firewall interfaces to a link-group.

```
<FW> system-view
[FW] interface GigabitEthernet 0/0/2
[FW-GigabitEthernet0/0/2] link-group 1
[FW] interface GigabitEthernet 0/0/3
[FW-GigabitEthernet0/0/3] link-group 1
```

- Check the status of link-group member interfaces.

```
[FW] display link-group 1
link group 1, total 2, fault 0
GigabitEthernet0/0/2 : up
GigabitEthernet0/0/3 : up
```

Contents

1. Overview of Firewall High Reliability Technologies
2. Firewall Hot Standby
3. Firewall Link High Reliability
4. **Hot Standby Version Upgrade and Troubleshooting**
 - Version Upgrade
 - Troubleshooting

Overview of the Hot Standby Version Upgrade

- Upgrading the hot standby system is one of the common O&M operations on the live network. The reasons for upgrading are as follows:

The software version on the live network has bugs that need to be fixed through the version upgrade.

The current software version on the live network does not support some features that are needed.

The software versions of the devices on the live network are inconsistent, and need to be unified.

- This course describes only the general roadmap for upgrading the hot standby system. Specific operations, including viewing device and service running information, backing up and comparing configuration files, uploading licenses and content security component packages, as well as verifying upgrade results, need to be adjusted based on live network conditions and requirements.
- Note that the version upgrade has requirements on the device model and source version. For details, see the related upgrade guide on Huawei official website.

Preparing for the Upgrade (1/4)

- Determine the upgrade mode: the web-based mode or the CLI-based mode.
- Prepare the upgrade environment, that is, configure the firewall as the web server or FTP server.
- Prepare the upgrade tools, including the login tool and configuration file comparison tool.
- Obtain the files required for the upgrade, such as the system software with the extension .bin, content security component packages, and local signature database upgrade packages.
- Check the running status of the device.
 - Check the current system software.
`<FW> display version`
 - Check the usage of the current license.
`<FW> display license`
 - Check the current hardware running status of the device.
`<FW> display device`

- Both web-based upgrade and CLI-based upgrade are applicable to the scenario where the device is running properly and carries service traffic.
- The two upgrade modes are supported in all upgrade scenarios. The CLI-based upgrade mode is recommended.
- Check the current configuration and running status of the device as well as the running status of services. Compare the configuration and running status with those after the upgrade to prevent service interruptions.

Preparing for the Upgrade (2/4)

- Query the current configuration file on the device.

```
<FW> display startup
```

- Check device interface information.

```
<FW> display interface brief
```

- Check the hot standby status of the device.

```
<FW> display hrp state  
<FW> display vrrp
```

- Check the service running status.

- Check the routing table of the device.

```
<FW> display ip routing-table
```

- Check the MAC address table of the device.

```
<FW> display mac-address
```

Preparing for the Upgrade (3/4)

- Check the session table of the device.

```
<FW> display firewall session table
```

- Check and back up important data.

- Back up the system software.

- Save the configuration and back up the configuration file.

```
<FW> save
```

```
ftp> get remote-filename [ local-filename ]
```

- Check the available space.

```
<FW> dir hda1:
```

Preparing for the Upgrade (4/4)

- Upload the target version software and set it as the software version for the next startup.

```
ftp> put local-filename [ remote-filename ]
```

```
<FW> startup system-software filename
```

Version Upgrade (1/2)

- To ensure service continuity during the upgrade, upgrade the system during off-peak hours, for example, non-working hours. In addition, upgrade the standby device first, and then the active device. Note that the HRP backup channel (heartbeat link) must be disconnected during the upgrade.
- Upgrading the standby device:
 1. Shut down the service interfaces of the standby device.
 2. Shut down the heartbeat interface of the standby device.
 3. Upgrade the system software version of the standby device.
 4. Run the **undo shutdown** command to enable the heartbeat interface of the standby device.
 5. Wait for the active and standby firewalls to synchronize entries including session entries.
 6. Run the **undo shutdown** command to enable the service interfaces of the standby device.
 7. Verify the upgrade result of the standby device, including checking the version information, license information, device running status, interface information, configurations, routing table, and session table.
 8. Save the configuration.

- You must shut down the service interfaces first and then the heartbeat interface. Otherwise, two active devices may exist.
- If services are abnormal after the upgrade, you need to roll back the version.

Version Upgrade (2/2)

- Upgrading the active device:
 1. Shut down the service interfaces of the active device.
 2. Shut down the heartbeat interface of the active device.
 3. Upgrade the system software version of the active device.
 4. Run the **undo shutdown** command to enable the heartbeat interface of the active device.
 5. Wait for the active and standby firewalls to synchronize entries including session entries.
 6. Run the **undo shutdown** command to enable the service interfaces of the active device.
 7. Verify the upgrade result of the active device, including checking the version information, license information, device running status, interface information, configurations, routing table, and session table.
 8. Save the configuration.

- If services are abnormal after the upgrade, you need to roll back the version.
- Note that when the HRP protocol format changes, the two system versions are incompatible. As a result, hot standby cannot be implemented, and two active devices may exist. In this case, run the **shutdown** command on the heartbeat interface of the active device, and then run the **undo shutdown** command on the heartbeat interface of the standby device. Service traffic is diverted to the standby device based on the VRRP priority.

Verifying the Upgrade

- Run the **display hrp state** command to view the service active/standby status of the firewall.
- Run the **Ping** command to test whether services are normal.
- Test the active/standby switchover.
 - Ping an Internet IP address from an intranet PC for a long time, shut down the uplink or downlink interface of the active firewall, and observe the firewall active/standby switchover and ping packet loss. If the switchover is successful, the standby firewall switches to the active device and carries services. The prefix before the command line prompt of the standby firewall changes from HRP_S to HRP_M, and the prefix before the command line prompt of the active firewall changes from HRP_M to HRP_S. Perform a ping test to check whether packet loss occurs.
 - Enable the uplink or downlink interface of the active firewall and observe the firewall active/standby switchover and ping packet loss. If the status switchover is successful, the active firewall switches to the active device and starts to carry service after the preemption delay (60s by default) expires. The prefix before the command line prompt of the active firewall changes from HRP_S to HRP_M, and the prefix before the command line prompt of the standby firewall changes from HRP_M to HRP_S. Perform a ping test to check whether packet loss occurs.

Contents

1. Overview of Firewall High Reliability Technologies
2. Firewall Hot Standby
3. Firewall Link High Reliability
4. **Hot Standby Version Upgrade and Troubleshooting**
 - Version Upgrade
 - Troubleshooting

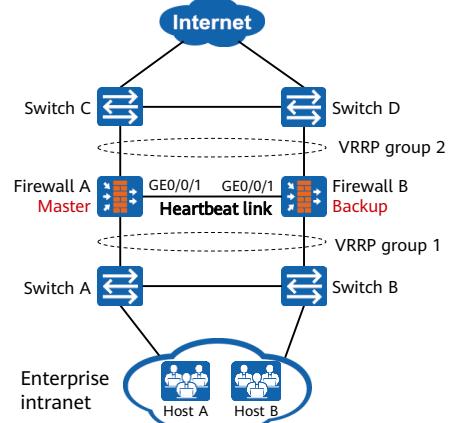
Fault 1: Abnormal HRP Status

- Symptom: In the active/standby firewall networking, the HRP running status of the peer end is **unknown** on Firewall A, as shown in the following command lines.

```
HRP_M[NGFW] display hrp state
Role: active, peer: unknown (should be "active-standby")
Running priority: 47004, peer: unknown
Core state: abnormal(active), peer: unknown
Backup channel usage: 0%
Stable time: 0 days, 3 hours, 48 minutes
```

- Fault cause analysis:
 - The hot standby function is not enabled on the peer device.
 - No backup channel is available.
- Solution:
 - Enable the hot standby function on the peer firewall.
 - Run the **display hrp interface** command to check the backup channel and rectify the fault if a fault exists.

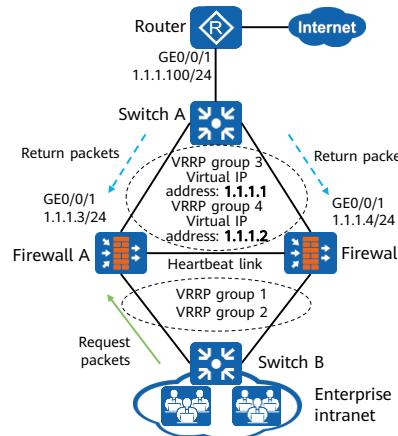
63 Huawei Confidential



 HUAWEI

Fault 2: Abnormal Traffic Forwarding Path in the NAT Scenario (1/2)

- Networking description: In the firewall load balancing networking scenario, both the upstream and downstream links use VRRP.
 - In VRRP groups 1 and 3, Firewall A is the active firewall and Firewall B is the standby firewall.
 - In VRRP groups 2 and 4, Firewall A is the standby firewall and Firewall B is the active firewall.
 - NAT address pool of Firewall A: 1.1.1.5 to 1.1.1.10.
 - NAT address pool of Firewall B: 1.1.1.11 to 1.1.1.15.
- Fault symptom: The return packets sent by the router sometimes reach Firewall A and sometimes reach Firewall B, affecting service running.



 HUAWEI

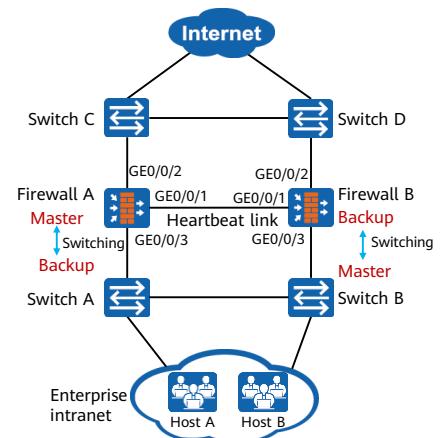
Fault 2: Abnormal Traffic Forwarding Path in the NAT Scenario (2/2)

- Fault cause analysis:
 - VRRP group 1 is used as an example. After traffic from intranet hosts to the Internet reaches Firewall A, the source IP address is changed to an Internet IP address (for example, 1.1.1.5) based on the NAT policy.
 - Firewall A synchronizes the NAT policy and NAT mapping information to Firewall B.
 - When sending a return packet, the router sends an ARP request querying the MAC address corresponding to the IP address 1.1.1.5. Both Firewall A and Firewall B will respond. As a result, the return traffic path is abnormal.
- Solution:
 - You need to bind the NAT address pool to the VRRP group on firewalls. The NAT address pool on Firewall A should be bound to VRRP group 3, and that on Firewall B should be bound to VRRP group 4.
 - After the binding, only Firewall A (active) responds to the ARP request, and the response MAC address is the virtual MAC address corresponding to VRRP group 3. All return traffic is forwarded only to Firewall A.

- The system can automatically bind the NAT address pool to the VRRP group with the smallest VRID if the NAT address pool and VRRP group reside on the same subnet. Therefore, in active/standby mode, you do not need to manually bind the NAT address pool to any VRRP groups.

Fault 3: Frequent Firewall Active/Standby Switchovers

- Symptom: In the active/standby networking scenario, the hot standby status of the firewall switches frequently, causing abnormal traffic.
- Fault cause analysis:
 - The service interfaces of the firewall frequently alternate between Up and Down. As a result, the active/standby switchovers occur frequently.
 - The intervals at which the active and standby firewalls send heartbeat packets are inconsistent.
- Solution:
 - Check whether the service interface configuration is correct.
 - If the service interface is an optical interface, check whether the optical module is normal.
 - Check the interval for sending heartbeat packets on the firewalls and ensure that the intervals are the same.



Quiz

1. (True or false) The heartbeat interfaces of firewalls can be directly connected or connected through switches or routers. ()
 - A. True
 - B. False
2. (Multiple-Answer question) Which of the following statements about the system version upgrade of the firewall hot standby are incorrect? ()
 - A. System upgrade is usually performed during off-peak hours.
 - B. In hot standby upgrade, the active device is upgraded first, and then the standby device.
 - C. Before the upgrade, back up important data such as configuration files.
 - D. You do not need to record the service running status before the upgrade because service status varies at different time.

1. A

2. BD

Summary

- This section describes firewall high reliability technologies, including hot standby and link high reliability technologies. Link high reliability technologies include Eth-Trunk, IP-Link, BFD, and Link-Group.
- In addition, this course describes common O&M operations of high reliability technologies, such as hot standby version upgrade and common troubleshooting.
- Upon completion of this course, you will be able to deploy and maintain high reliability technologies on firewalls and can meet high reliability requirements of medium- and large-sized enterprise networks.

Recommendations

- Huawei official websites:
 - Enterprise service: <https://e.huawei.com/en/>
 - Technical support: <https://support.huawei.com/enterprise/en/index.html>
 - Online learning: <https://www.huawei.com/en/learning>

Acronyms and Abbreviations (1/2)

Acronym/Abbreviation	Full Name
ARP	Address Resolution Protocol
BFD	Bidirectional Forwarding Detection
HRP	Huawei Redundancy Protocol
ICMP	Internet Control Message Protocol
LACP	Link Aggregation Control Protocol
LAG	Link Aggregation Group
MAC	Media Access Control
NO-PAT	No-port Address Translation
OSPF	Open Shortest Path First
PAT	Port Address Translation

Acronyms and Abbreviations (2/2)

Acronym/Abbreviation	Full Name
POS	Packet Over SDH/SONET
USG	Unified Security Gateway
VLAN	Virtual Local Area Network
VGMP	VRRP Group Management Protocol
VRRP	Virtual Router Redundancy Protocol
VPN	Virtual Private Network

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。
Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

Copyright©2022 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product performance, market position, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.



Firewall Traffic Management



Foreword

- As the limited network bandwidth cannot cope with the ever-increasing network services, efficient bandwidth management is required to ensure that high-priority services are preferentially forwarded while limiting the bandwidth resources used by low-priority services. Due to coarse traffic classification, traditional traffic management, however, cannot manage traffic hierarchically, failing to meet current user requirements.
- Huawei's firewall traffic management technology consists of bandwidth management and quota control policies. The technology is applicable to the multiple organizational structures as it can accurately identify and manage service traffic and provide hierarchical traffic policies. This course describes traffic management technologies in detail.

Objectives

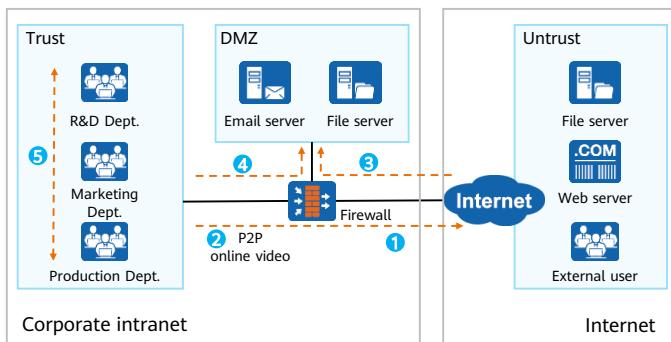
- On completion of this course, you will be able to:
 - Describe the application scenarios of bandwidth management.
 - Describe the fundamentals of bandwidth management.
 - Describe the application scenarios of quota control policies.
 - Describe the fundamentals of quota control policies.
 - Master the configurations of firewall traffic management.

Contents

- 1. Firewall Bandwidth Management**
2. Firewall Quota Control Policies
3. Example for Configuring Traffic Management

Background of Bandwidth Management

- As the egress gateways of large and medium-sized enterprises, firewalls are deployed at the network border to limit incoming and outgoing traffic. Non-critical service traffic occupies a large amount of bandwidth, which brings a series of problems to enterprises. For example, the server cannot be accessed, employee's work efficiency is low, and the server performance deteriorates.



- ① Internet access from intranet users requires massive bandwidth.
- ② P2P services consume most of bandwidth resources.
- ③ Massive Internet traffic destined for intranet servers deteriorates server performance.
- ④ A large number of access requests flood the intranet servers, causing them to malfunction.
- ⑤ Different users or departments overuse bandwidth resources, which deteriorates network quality.

Overview of Bandwidth Management

- For enterprise user traffic, the firewall provides the bandwidth management function to manage and control traffic based on the inbound/outbound interfaces, source/destination security zones, source/destination addresses, schedules, and DSCP priorities.
- Bandwidth management enables the firewall to limit bandwidth, guarantee bandwidth, and limit the maximum number of connections to improve bandwidth efficiency and prevent bandwidth exhaustion.

Bandwidth limit

Bandwidth assurance

Connection limit

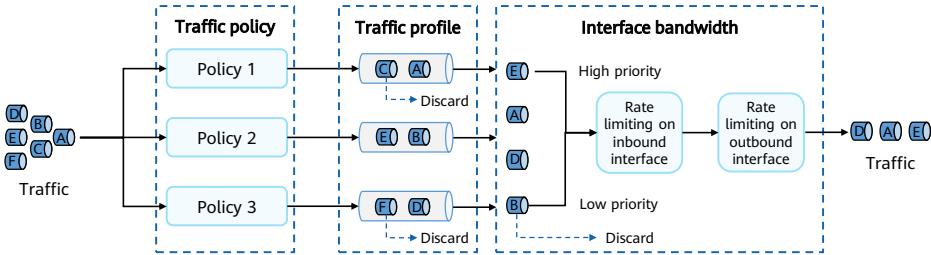
- The firewall limits the bandwidth of non-critical services on the network to prevent them from consuming large amounts of bandwidth and affecting other services.

- The firewall guarantees sufficient bandwidth for critical services transmitted over a busy link.

- The firewall limits the number of connections for a specific service to prevent this service from overusing bandwidth resources and save session resources.

Bandwidth Management Process

- The firewall implements bandwidth management through traffic policies, traffic profiles, and interface bandwidth.
 - Traffic policy: defines the managed objects and traffic actions and references a traffic profile.
 - Traffic profile: defines the bandwidth resources to be used by managed objects.
 - Interface bandwidth: defines the actual bandwidth in the inbound and outbound directions of an interface. When congestion occurs in the outbound direction, the queue scheduling mechanism is enabled.



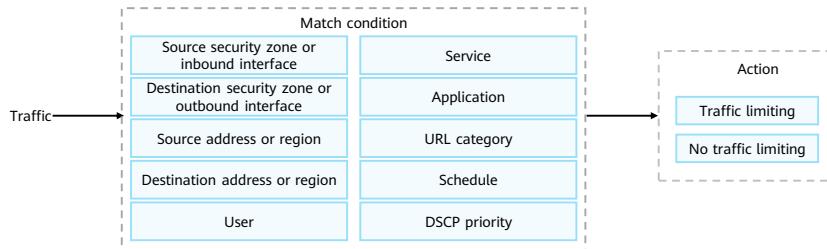
6 Huawei Confidential

 HUAWEI

- The general bandwidth management process is as follows:
 - The firewall implements traffic policies to match and classify traffic for multiple traffic profiles. The processing in the traffic profiles includes:
 - Discards the traffic that exceeds the predefined maximum bandwidth.
 - Limits the number of connections for services.
 - Marks traffic priorities for follow-up queue scheduling.
 - On the inbound interface, if the traffic volume exceeds the inbound interface bandwidth, the bandwidth management schedules all traffic based on the forwarding priorities specified in traffic profiles and preferentially forwards the high-priority traffic.
 - The bandwidth management also limits outgoing traffic based on the outbound interface bandwidth. If the traffic volume exceeds the outbound interface bandwidth, the bandwidth management schedules all traffic based on the forwarding priorities specified in traffic profiles and preferentially forwards the high-priority traffic.

Traffic Policy Rules

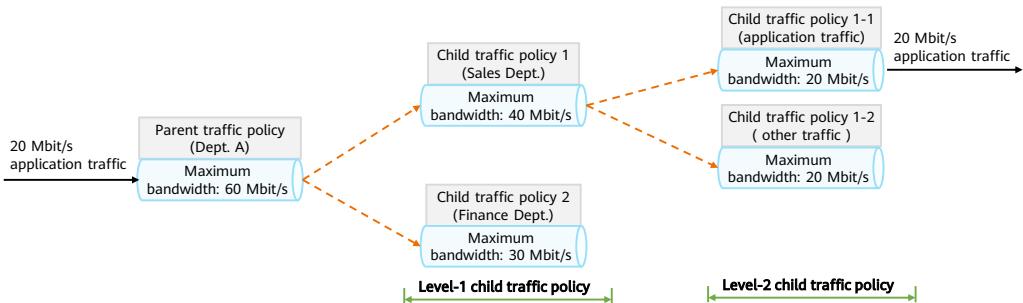
- Traffic policies determine which traffic on the network requires bandwidth management and how bandwidth management is implemented.
- A traffic policy is a collection of multiple traffic policy rules, with each rule containing specific conditions and actions.
 - A condition is the basis for matching packets.
 - An action indicates how a firewall processes packets that match conditions:
 - Traffic limiting: rate-limits the traffic that meets the conditions. When the action of a traffic policy is traffic limiting, it needs to reference a traffic profile, which determines specific management measures on the traffic.
 - No traffic limiting: does not rate-limit the traffic that meets the conditions.



- There is a default traffic policy on the firewall. All matching conditions are any, and the action is no traffic limiting. If no policy is matched on the firewall, the default traffic policy is used.

Traffic Policy Types

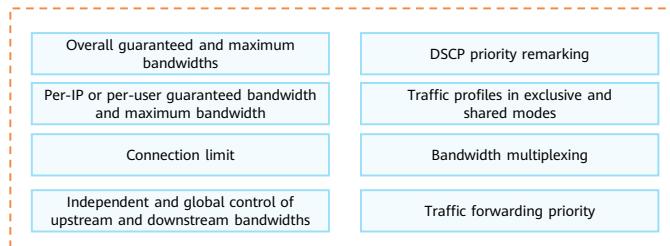
- Multiple traffic policies can be configured on a firewall. The following two types of traffic policies are used in most cases:
 - Same-level policy: Multiple traffic policies are independent of each other. The firewall matches the traffic against multiple policies of the same level from top to bottom. Once the traffic matches all conditions of a policy, the action of the referenced traffic profile is performed immediately and the policy matching stops.
 - Hierarchical policy: It is also called parent-child policy. That is, multiple traffic sub-policies can be configured under a traffic policy. For hierarchical policies, traffic is always matched against a parent policy before child policies.



- When traffic policies are implemented, you can configure hierarchical policies to achieve better bandwidth multiplexing. Currently, the firewall running V6R7C20 supports four-level hierarchical policies.
- As shown in the preceding figure, when the 20 Mbit/s application traffic matches the traffic policy, the process is as follows:
 - The traffic matches the parent policy first. If the traffic bandwidth is lower than the maximum bandwidth (60 Mbit/s) of the parent policy, the traffic needs to match the level-1 child policy. Otherwise, the traffic is discarded.
 - The traffic bandwidth is lower than the maximum bandwidth (40 Mbit/s) of the matched child policy 1, and the level-2 child policy needs to be matched. Otherwise, the matching fails.
 - The traffic bandwidth is lower than the maximum bandwidth (20 Mbit/s) of the matched child policy 1-1, all traffic is forwarded. If the application traffic is higher than 20 Mbit/s, the application rate will be limited to 20 Mbit/s.

Traffic Profile

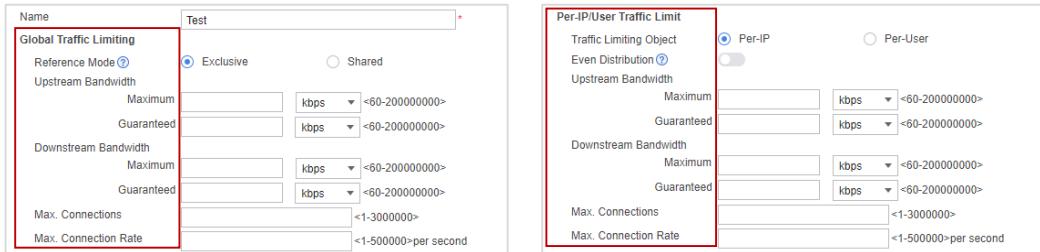
- A traffic profile defines the availability of bandwidth resources. The firewall applies a traffic profile to traffic that matches the specific traffic policy.
- A traffic profile on the firewall can logically divide physical bandwidth resources into multiple virtual bandwidth resources. A traffic profile limits bandwidth resources from the following aspects: overall guaranteed bandwidth and maximum bandwidth, per-IP or per-user maximum bandwidth, connection limit, and DSCP priority remarking. The traffic profile also implements bandwidth multiplexing during off-peak hours.



- Overall guaranteed bandwidth and maximum bandwidths: They indicate the minimum and maximum bandwidth resources that can be allocated for the traffic to which the traffic profile is applied.
- Per-IP or per-user guaranteed bandwidth and maximum bandwidth: The minimum bandwidth and maximum bandwidth are set for each IP address or user in the traffic profile to implement fine-grained bandwidth control.
- Connection limit: The firewall limits the number of connections by limiting the number of sessions generated by itself.
- Independent and global control of upstream and downstream bandwidths: The maximum bandwidth, guaranteed bandwidth, and connection limit can be configured separately for upstream and downstream traffic. In a traffic profile, the meanings of upstream and downstream traffic are related to the traffic policy.
 - If the traffic transmission direction is the same as that specified in the traffic policy, the traffic is defined as upstream traffic.
 - Otherwise, the traffic is defined as downstream traffic.
- DSCP priority remarking: The DSCP field, also called DSCP priority, is the basis for network devices to classify traffic. The firewall can change the DSCP field value of the packets that meet the conditions in the traffic profile, and then process the traffic with different DSCP priorities in different ways.
- Bandwidth multiplexing: After multiple traffic flows enter the same traffic profile, the bandwidth resources in the traffic profile can be dynamically allocated for them.
- Traffic forwarding priority: The firewall supports the configuration of traffic forwarding priorities for traffic profiles. Different priorities correspond to two bandwidth limiting modes: traffic policing and traffic shaping.

Setting Traffic Profile Parameters

- The bandwidth setting includes the following important parameters:
 - Overall guaranteed and maximum bandwidths
 - Per-IP or per-user guaranteed bandwidth and maximum bandwidth
 - Independent and global control of upstream and downstream bandwidths
 - Connection limit (concurrent connection limit and new connection rate limit)



10 Huawei Confidential

HUAWEI

- The overall guaranteed bandwidth is the minimum available bandwidth assigned by a traffic profile to traffic that matches the traffic profile. Similarly, the overall maximum bandwidth is the maximum available bandwidth assigned by a traffic profile to traffic that matches the traffic profile. After traffic enters a traffic profile, the firewall compares the current traffic with the guaranteed/maximum bandwidth set in the traffic profile and processes the traffic in different ways:
 - If the traffic requires bandwidth lower than the guaranteed bandwidth, the firewall directly forwards it on the outbound interface.
 - If the traffic requires bandwidth higher than the maximum bandwidth, the firewall discards the excess traffic.
 - If traffic requires bandwidth higher than the guaranteed bandwidth, the traffic competes for bandwidth resources with the same type of traffic that is processed using other traffic profiles. Traffic with higher priority has a better chance to be forwarded than those with lower priority. Traffic is sent after bandwidth resources are obtained. Otherwise, the traffic is discarded.
- Per-IP or per-user guaranteed bandwidth and maximum bandwidth: In addition to the overall guaranteed bandwidth and maximum bandwidth, the per-IP or per-user guaranteed bandwidth and maximum bandwidth can be specified in a traffic profile for refined bandwidth restriction.
 - After traffic policies reference traffic profiles, the firewall collects statistics on traffic matching traffic policies based on IP addresses or users. The function of the per-IP or per-user guaranteed bandwidth and maximum bandwidth is similar to that of the global bandwidth. The difference is that the guaranteed bandwidth and maximum bandwidth is subject to an IP address or user.

- In addition, the firewall can dynamically and equally distribute bandwidth resources to each IP address or user based on the global maximum bandwidth and the number of online IP addresses or users, fully utilizing bandwidth resources.
- Connection limit: The connection established between two communication parties is a session on the firewall. One session corresponds to one connection. The firewall limits the connections by limiting the sessions created by itself. The main functions include the following:
 - P2P services generate a large number of connections. Limiting the number of connections helps reduce P2P service traffic and bandwidth consumption.
 - In the scenario where an internal network server is deployed, limiting the connections can help the firewall to prevent the Distributed Denial Of Service (DDoS) attack on the internal network server.
 - The session resources on the firewall are saved.
- The maximum number of global connections and the maximum number of source-IP-address-specific or user-specific connections can be set in a traffic profile.
- Independent and global control of upstream and downstream bandwidths: The maximum bandwidth, guaranteed bandwidth, and connection limit can be configured separately for upstream and downstream traffic. In a traffic profile, the upstream and downstream directions have specific mapping relationship with the traffic policy to which the traffic profile is referenced. If the direction is the same as that of the traffic policy, the direction is upstream. If not, the direction is downstream. That is, if a traffic flow matches the traffic policy, the traffic is upstream traffic. If the source and destination in the traffic policy are exchanged, the matched traffic is downstream traffic.
- For example, you can configure either of the following methods to limit the traffic from the Trust zone to the Untrust zone:
 - When the source zone of the traffic policy is Trust and the destination zone is Untrust, configure upstream bandwidth control in the traffic profile (same direction as the traffic policy).
 - When the source zone of the traffic policy is Untrust and the destination zone is Trust, configure downstream bandwidth control in the traffic profile (reverse direction of the traffic policy).
- In addition, the firewall supports bandwidth control based on the total of upstream and downstream traffic.

Working Modes

- After a traffic policy references a traffic profile, the overall maximum bandwidth, guaranteed bandwidth, and maximum number of connections defined in a traffic profile take effect on the traffic that matches the policy. A traffic profile works in either of the following modes:

Exclusive mode

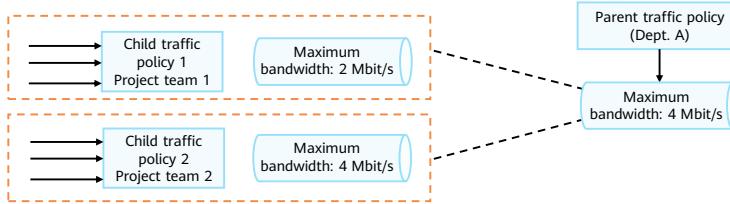
- A traffic profile is used by only one policy. Traffic that matches the policy has exclusive use of the maximum bandwidth defined in the traffic profile.

Shared mode

- A traffic profile is shared by multiple traffic policies. Traffic that matches these traffic policies shares the maximum bandwidth defined in the traffic profile.

Bandwidth multiplexing

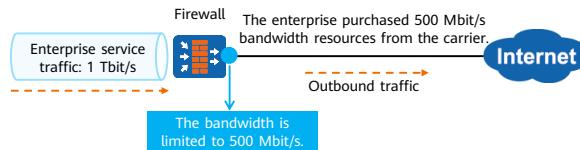
- Bandwidth multiplexing serves as an important feature of a traffic profile. It refers to the dynamic allocation mode of bandwidth resources in a traffic profile after multiple traffic flows enter the same traffic profile. If a traffic flow does not use bandwidth resources, other flows can borrow the idle resources. If a traffic flow needs bandwidth resources, the flow can preempt bandwidth resources.
- Bandwidth multiplexing applies to the following scenarios:
 - Traffic flows matching the same traffic policy can share bandwidth resources.
 - If multiple traffic policies reference a traffic profile in policy shared mode, bandwidth multiplexing can be implemented among multiple traffic flows that match the traffic policy.
 - Bandwidth multiplexing can be implemented among multiple traffic flows that match multiple child policies in the parent and child policies.



- Compared with an independent traffic policy, a hierarchical policy can enable bandwidth multiplexing to function better.
- For example, department A has two project teams: project team 1 and project team 2. A parent policy is used to limit the maximum bandwidth of department A, and two child policies to limit that of the two project teams. If project team 2 (child policy 2) has only 2 Mbit/s traffic, project team 1 (child policy 1) can use the remaining 2 Mbit/s bandwidth resources of department A (parent policy). Without the hierarchical policy, each team can use only the amount of bandwidth allowed by its own child policy, and the bandwidth resources of department A cannot be multiplexed.

Interface Bandwidth Principle

- When a firewall functions as the egress gateway of a large and midsize enterprise, the bandwidth that the enterprise purchases from the carrier is generally less than the physical bandwidth of the outbound interface on the firewall. If maximum available bandwidth is not set on the outbound interface, the bandwidth required by traffic may exceed the available bandwidth on the outbound interface. As a result, traffic congestion occurs and packets may be discarded on the peer devices.
- An enterprise can set the maximum bandwidth of an outbound interface to less than or equal to the bandwidth purchased from the carrier. If traffic exceeds the maximum available bandwidth on the outbound interface, the firewall can detect traffic congestion and trigger queue scheduling to ensure that packets with higher priorities are forwarded preferentially. In addition, the enterprise can set the actual bandwidth limit on the inbound interface. When the firewall receives traffic from other devices, it limits the traffic entering the interface to prevent performance deterioration caused by heavy pressure on the internal server.

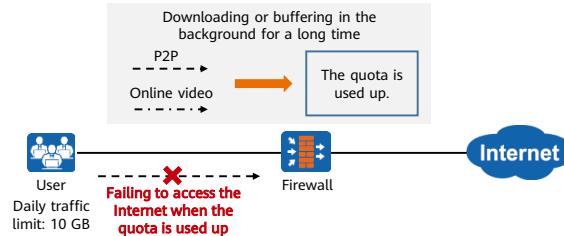


Contents

1. Firewall Bandwidth Management
- 2. Firewall Quota Control Policies**
3. Example for Configuring Traffic Management

Overview of Quota Control Policy

- Bandwidth management can solve most of the preceding issues. However, entertainment traffic still brings the following issues:
 - A small number of employees use P2P download and online video applications. These applications consume almost all bandwidth resources of the enterprise, leaving insufficient bandwidth for key services.
 - Enterprises whose settlement expenditure is based on traffic and ISP can no longer leverage the traditional bandwidth limiting mode to deal with activities such as slow but prolonged P2P downloads and caching.
 - Employees use the Internet to carry out entertainment activities for a long time, which severely affects their work efficiency.



Principles of Quota Control Policies

- Quota control policies control users' online traffic and online duration to avoid bandwidth overuse and impact on work efficiency due to long online duration. Quota control policies include the following types:
 - Detection: Detect the real-time Internet access traffic and duration and compare them with the Internet access quota of the user. The comparison result serves as the reference for further control.
 - Control: Directly block traffic or limit the maximum bandwidth.



17 Huawei Confidential

 HUAWEI

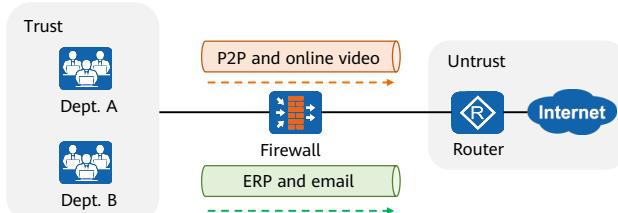
- Administrators can provide three quota allocation modes for users to facilitate diversified management.
 - Daily traffic quota: specifies the total daily Internet access traffic of a user.
 - Monthly traffic quota: specifies the total monthly Internet access traffic of a user.
 - Daily Internet access duration quota: specifies the total daily Internet access duration of a user.

Contents

1. Firewall Bandwidth Management
2. Firewall Quota Control Policies
3. **Example for Configuring Traffic Management**

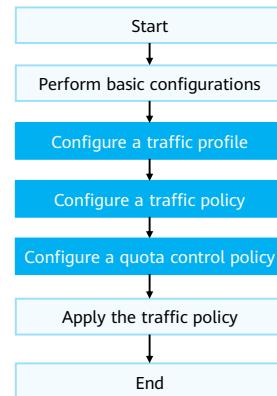
Example for Configuring Traffic Management (1/2)

- Requirement description:
 - An enterprise purchases 100 Mbit/s bandwidth from the ISP. The maximum downstream bandwidth of department A cannot exceed 60 Mbit/s, and that of department B cannot exceed 40 Mbit/s.
 - The maximum downstream P2P bandwidth of departments A and B cannot exceed 30 Mbit/s, and the P2P bandwidth needs to be included in the total bandwidth of each department. To better control P2P and online video traffic, you can set the number of connections to a maximum of 10,000. To improve employees' work efficiency, each user can use a maximum of 15 GB P2P and online video traffic per month.
 - To ensure that applications such as email and ERP are not affected during working hours, the minimum bandwidth for such traffic must be no less than 30 Mbit/s, and the traffic must be included in the total traffic of each department.



Example for Configuring Traffic Management (2/2)

- Configuration roadmap:
 - Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
 - Limit the maximum downstream bandwidth of each department based on the company's requirements.
 - Configure a traffic policy for P2P and online video applications and reference the traffic profile in which the overall maximum bandwidth is 30 Mbit/s and overall maximum number of connections is 10,000.
 - Configure the bandwidth limit for email and ERP applications and set the guaranteed bandwidth.
 - Configure a quota control policy to limit the monthly P2P traffic of a user.



Department Bandwidth Limit - Configuring a Traffic Profile

- Configure a traffic profile for department A. Choose **Policy > Bandwidth Management > Traffic Profile**, click **Add**, and set the parameters as shown in the following figure.

The screenshot shows the 'Add Traffic Profile' configuration interface. Key settings include:

- Name:** profile_dep_a (highlighted by red box 1)
- Reference Mode:** Exclusive (highlighted by red box 2)
- Upstream Bandwidth:** Maximum: 60 Mbps (highlighted by red box 3)
- Downstream Bandwidth:** Maximum: 60 Mbps (highlighted by red box 3)
- Max. Connections:** Empty
- Max. Connection Rate:** Empty

Department Bandwidth Limit - Configuring a Traffic Policy

- To manage the bandwidth for department A, choose **Policy > Bandwidth Management > Traffic Policy**, click **Add**, and set the parameters as shown in the figure on the right.

The screenshot shows the 'Add Traffic Policy' configuration page. Key fields and their values are highlighted with red boxes and numbered 1 through 4:

- Name:** policy_dep_a (highlighted by red box 1)
- Source Type:** Inbound Interface (highlighted by red box 2)
- Destination Type:** Source Zone (highlighted by red box 3)
- Action:** Limit (highlighted by red box 4)
- Traffic Profile:** profile_dep_a (highlighted by red box 4)

22 Huawei Confidential



- Similarly, a traffic policy needs to be configured for department B.

P2P Bandwidth Limit - Configuring a Traffic Profile

- Configure traffic profiles for the P2P applications of departments A and B. Choose **Policy > Bandwidth Management > Traffic Profile**, click **Add**, and set the parameters as shown in the following figure.

Add Traffic Profile

Name	① profile_p2p_all *
Global Traffic Limiting	<input type="radio"/> Exclusive <input checked="" type="radio"/> Shared
Upstream Bandwidth	Maximum <input type="text"/> kbps <60-200000000> Guaranteed <input type="text"/> kbps <60-200000000>
Downstream Bandwidth	Maximum <input type="text" value="30"/> Mbps <1-200000> Guaranteed <input type="text"/> Mbps <1-200000>
Max. Connections	④ 10000 <1-3000000>
Max. Connection Rate	<input type="text"/> <1-500000>per second

P2P Bandwidth Limit - Configuring a Traffic Policy

- To manage the bandwidth of P2P applications for department A, choose **Policy > Bandwidth Management > Traffic Policy**, click **Add**, and set the parameters as shown in the figure on the right.

The screenshot shows the 'Add Traffic Policy' configuration page. The 'Name' field is filled with 'policy_dep_a_p2p'. The 'Destination Type' dropdown is set to 'untrust'. The 'Application' dropdown is set to 'P2P-Based'. The 'Action' dropdown is set to 'Limit' with the profile 'profile_p2p_all' selected. Red numbers 1 through 4 are overlaid on the interface to point to specific fields: 1 points to the 'Name' field, 2 points to the 'Destination Type' dropdown, 3 points to the 'Application' dropdown, and 4 points to the 'Action' dropdown.

24 Huawei Confidential



- Similarly, a traffic policy needs to be configured for P2P applications in department B.
- Note: P2P-based applications are provided as an example. Specify the applications based on the actual requirements.

Bandwidth Limit for Email and ERP Applications - Configuring a Traffic Profile

- Configure schedule for Email and ERP applications.
- To configure traffic profiles for the email and ERP applications, choose **Policy > Bandwidth Management > Traffic Profile**, click **Add**, and set the parameters as shown in the following figure.

The figure shows two configuration panels side-by-side:

Global Traffic Limiting Panel:

- Name: profile_email (highlighted with red box ①)
- Reference Mode: Shared (highlighted with red box ②)
- Upstream Bandwidth:
 - Maximum: 60 Gbps
 - Guaranteed: 60 Gbps
- Downstream Bandwidth:
 - Maximum: 1.2 Gbps
 - Guaranteed: 30 Mbps (highlighted with red box ③)
- Max. Connections: 300,000
- Max. Connection Rate: 5,000,000 per second

Schedule Panel:

- Type: Periodic
- Start Time: 08:30:00
- End Time: 18:00:00
- Weekly Validity Time: Monday, Tuesday, Wednesday, Thursday, Friday (highlighted with red box)

Buttons at the bottom: OK (blue) and Cancel (gray).

Bandwidth Limit for Email and ERP Applications - Configuring a Traffic Policy

- To manage bandwidth for email and ERP applications, choose **Policy > Bandwidth Management > Traffic Policy**, click **Add**, and set the parameters as shown in the figure on the right.

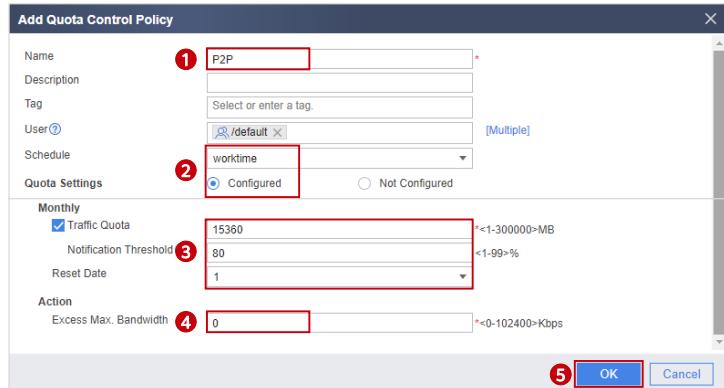
The screenshot shows a configuration form for a traffic policy. The fields are numbered 1 through 5:

- Name:** policy_dep_a_email (highlighted with a red box)
- Tag:** Select or enter a tag. (highlighted with a red box)
- Parent Policy:** policy_dep_a
- Source Type:** Inbound Interface (radio button) (highlighted with a red box)
- Source Zone:** Source Zone (radio button) (highlighted with a red box)
- Destination Type:** Outbound Interface (radio button) (highlighted with a red box)
- Destination Zone:** Destination Zone (radio button) (highlighted with a red box)
- Source Address/Region:** trust (highlighted with a red box)
- Destination Address/Region:** untrust (highlighted with a red box)
- User:** Select or enter a user name.
- Service:** Select or enter a service.
- Application:** Outlook, LotusNotes (highlighted with a red box)
- URL Category:** Select or enter a url category.
- Schedule:** worktime (highlighted with a red box)
- DSCP Value:** any
- Action:** Limit (radio button) (highlighted with a red box)
- Traffic Profile:** profile_email (highlighted with a red box)

- The above example describes the bandwidth management configuration for Outlook Web Access and LotusNotes. You can specify other services as required.

Quota Control Policy

- To configure a quota control policy for all users in a user group, choose **Policy > Quota Control Policy**, click **Add**, and set the parameters as shown in the following figure.



Quiz

1. (True or False) In bandwidth management, the guaranteed bandwidth can be greater than the maximum bandwidth. ()
 - A. True
 - B. False
2. (Multiple-Answer Question) An traffic policy rule consists of conditions and actions. Which of the following are matching conditions of a traffic policy rule? ()
 - A. Source security zone or inbound interface
 - B. User
 - C. Service
 - D. Schedule

1. B
2. ABCD

Summary

- This course describes the basic concepts and process of bandwidth management, including the traffic policy, traffic profile, and interface bandwidth. However, in special scenarios, bandwidth management may fail to meet enterprise requirements. Therefore, quota control policies can be used to limit user traffic.
- Upon completion of this course, you have mastered the basic configuration of firewall traffic management, helping users identify services and manage traffic more accurately.

Recommendations

- Huawei official websites:
 - Enterprise service: <https://e.huawei.com/en/>
 - Technical support: <https://support.huawei.com/enterprise/en/index.html>
 - Online learning: <http://learning.huawei.com/en/>

Acronyms and Abbreviations

Acronym/Abbreviation	Full Name
DDoS	Distributed Denial of Service
DMZ	Demilitarized Zone
DSCP	Differentiated Services Code Point
ERP	Enterprise Resource Planning
IP	Internet Protocol
ISP	Internet service provider
P2P	Peer to Peer
URL	Uniform Resource Locator

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。
Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

Copyright©2022 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product performance, market position, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.



Firewall Virtual System



 HUAWEI

Foreword

- As the network scale expands, the network environment of enterprises becomes more and more complex. Traditional physical network isolation solutions cannot meet users' requirements for service and application isolation. For example, management is scattered, security policies are difficult to deploy, and unified application services cannot be provided. To meet service and application isolation requirements and reduce investment costs, the concept of using a single gateway to function as multiple gateways is proposed. In this case, the virtual system (vSYS) technology emerges.
- This course describes the applications and fundamentals of firewall virtualization technology.

Objectives

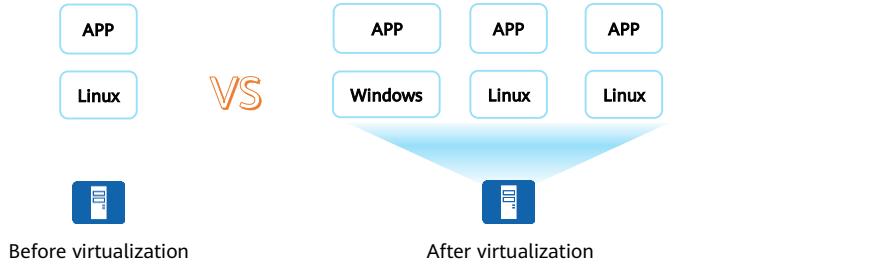
- Upon completion of this course, you will be able to:
 - Describe the application scenarios of virtual systems.
 - Describe the basic concepts of virtual systems.
 - Master how to configure virtual systems.

Contents

- 1. Virtual System Overview**
2. Basic Concepts of Virtual Systems
3. Communication Between Virtual Systems
4. Virtual System Configuration

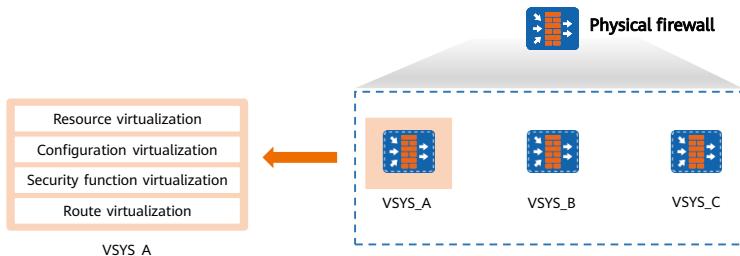
Virtualization Overview

- In a broad sense, virtualization refers to any technology that abstracts resources from one form into another. In a narrow sense, virtualization refers to logical abstraction of resources so that resource allocation is free from physical restrictions.
- Virtualization allows multiple VMs to run on a physical server. The VMs share the CPU, memory, and I/O hardware resources of the physical server, but are logically isolated from each other. Virtualization can reduce hardware costs, power consumption, and space.



Firewall Virtual System

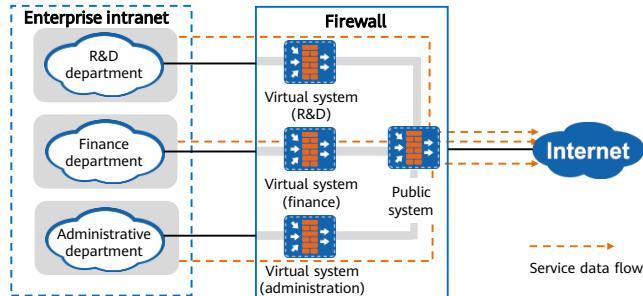
- A physical firewall can be logically divided into multiple virtual systems, which are isolated from each other. Every virtual system has its own interfaces, address sets, users or user groups, routing entries, and policies. It can be configured and managed by the virtual system administrator.



- The following virtualization functions are implemented by the firewall in order to forward, isolate, and independently manage traffic of different virtual systems?
 - Resource virtualization: Each virtual system has its own resources, including interfaces, VLANs, policies, and sessions. The resources are assigned by the public system administrator and managed by corresponding virtual system administrators.
 - Configuration virtualization: Each virtual system has its own administrator and configuration interface and cannot be accessed by administrators of other virtual systems.
 - Security function virtualization: Each virtual system has its own security policies and other security functions, which apply only to packets of the virtual system.
 - Route virtualization: Each virtual system maintains its own routing table, which is isolated from the routing tables of other virtual systems. Currently, only static routes can be virtualized.
- With the preceding virtualization functions, each virtual system can function as a logical firewall on a physical firewall and is exclusively managed by its administrator.

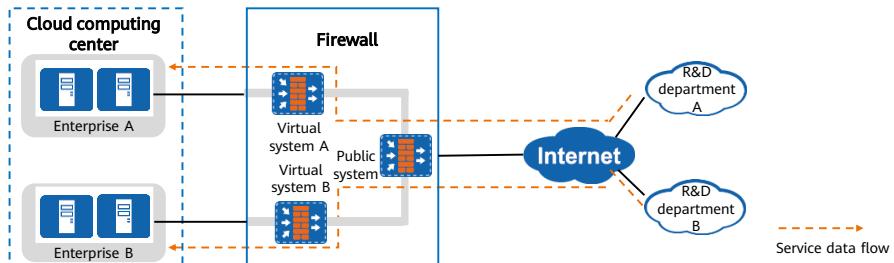
Virtual System Application Scenarios - Network Isolation for Large and Midsize Enterprises

- Large and midsize enterprises usually have a large number of network devices and complex network environments. As the enterprise service scale increases, the functions, permissions, and responsibilities of each service department become clearer. Each department has different security requirements. As a result, the firewall configuration is complex and the administrator's operations are prone to errors. The firewall virtualization technology allows you to divide a network into multiple subnets and configure a virtual system for each subnet, making network boundaries clearer and network management easier.
- As shown in the figure, virtual systems are created on the firewall for the R&D, finance, and administrative departments of an enterprise. The rights of virtual system administrators for different departments are different, and employees in different departments can access each other based on policies.



Virtual System Application Scenarios - Cloud Computing Security Gateway

- Cloud computing provides network resources and computing capabilities on the cloud. Network users can access related network resources and use corresponding services after connecting to the Internet through terminals. In this process, traffic isolation between users, security protection, and resource allocation are important. The virtual system technology grants cloud computing gateway capabilities to the firewall deployed at the egress of a cloud computing center. The firewall can then isolate user traffic and provide effective security protection.
- As shown in the figure, enterprises A and B have servers in the cloud computing center. The firewall functions as the security gateway at the egress of the cloud computing center. It isolates the networks and traffic of different enterprises and protects the cloud computing center based on the configured security policies.



Contents

1. Virtual System Overview
2. **Basic Concepts of Virtual Systems**
 - Independent Virtual System Management
 - Virtual System Resource Allocation
 - Virtual System Traffic Isolation
 - Independent Virtual System Configuration
3. Communication Between Virtual Systems
4. Virtual System Configuration

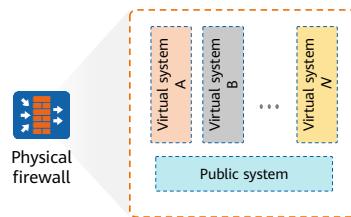
Virtual System Features

- After resources, configurations, security functions, and routes on a firewall are virtualized, service traffic of virtual systems can be correctly forwarded and isolated from each other. A virtual system has the following features:

Independent management	Resource allocation	Traffic isolation	Independent configuration
<ul style="list-style-type: none">Each virtual system is managed by its own administrator, which simplifies the management of multiple virtual systems and is suitable for large-scale networking.	<ul style="list-style-type: none">Each virtual system has its own resource quota so that a busy virtual system has no impact on other virtual systems.	<ul style="list-style-type: none">The traffic of different virtual systems is isolated to ensure security. However, different virtual systems can still communicate with each other if needed.	<ul style="list-style-type: none">Each virtual system has its own configurations and routing entries so that LANs connected to different virtual systems can communicate with each other even if the LANs use the same address range.

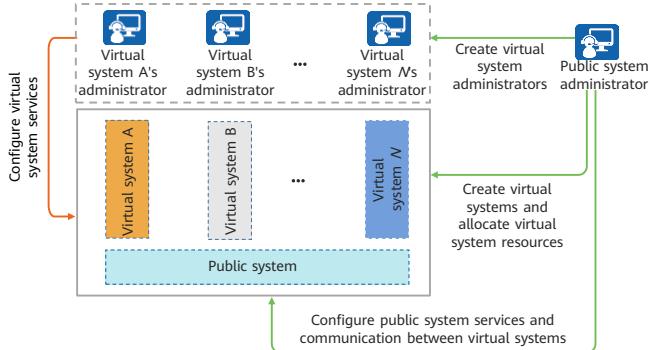
Virtual System Types

- A firewall has two types of virtual systems: public system and virtual system.
 - Public system
 - The public system is a default special virtual system on the firewall. The public system exists even if the virtual system function is disabled and configuring the firewall is equivalent to configuring the public system in this scenario. After the virtual system function is enabled, the public system inherits all configurations of the firewall.
 - The public system manages other virtual systems and forwards data between them.
 - Virtual system
 - A virtual system is an independent logical firewall created on a physical firewall.



Virtual System Management

- Each virtual system is independently managed and configured and has its own administrator. Based on the virtual system type, administrators are classified into public system administrators and virtual system administrators. The two types of administrators have different permissions.



11 Huawei Confidential

HUAWEI

- Public system administrator

- After the virtual system function is enabled, the device administrator will become the public system administrator, with login and authentication modes as well as management permissions remaining unchanged. The public system administrator manages and maintains the device and configures services of the public system.
- The public system administrator, who has the virtual system management permission, can configure virtual systems, such as creating or deleting virtual systems, and allocating resources to virtual systems.

- Virtual system administrator

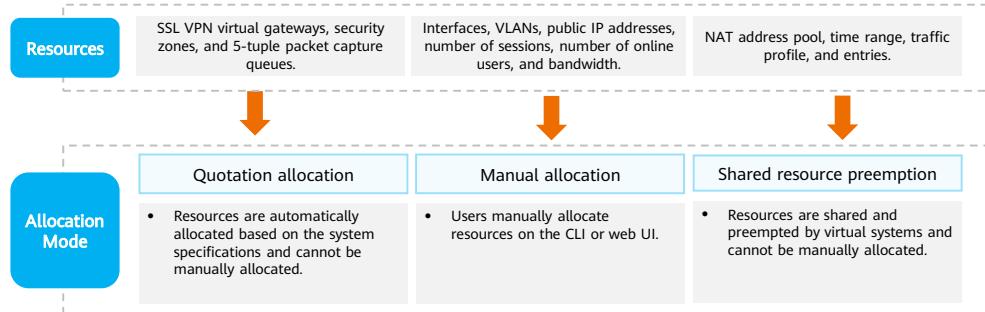
- Once a virtual system is created, the public system administrator can configure one or more administrators for it. The permissions of a virtual system administrator differ from those of a public system administrator: The administrator of a virtual system can access only the configuration page of the virtual system, and configure and view the virtual system's services. The public system administrator can access the configuration pages of all virtual systems and configure services for all virtual systems.
- To correctly identify the virtual system to which each administrator belongs, name virtual system administrator accounts in the format of Administrator name@@Virtual system name.

Contents

1. Virtual System Overview
2. **Basic Concepts of Virtual Systems**
 - Independent Virtual System Management
 - **Virtual System Resource Allocation**
 - Virtual System Traffic Isolation
 - Independent Virtual System Configuration
3. Communication Between Virtual Systems
4. Virtual System Configuration

Resource Allocation

- If a virtual system uses too many resources, other virtual systems cannot obtain resources and their services cannot run properly. Proper resource allocation prevents a virtual system from occupying too many resources.
- Basic resources for virtual system services can be allocated manually or based on quotas. Other resources are shared and preempted. Different resources are allocated in different ways.

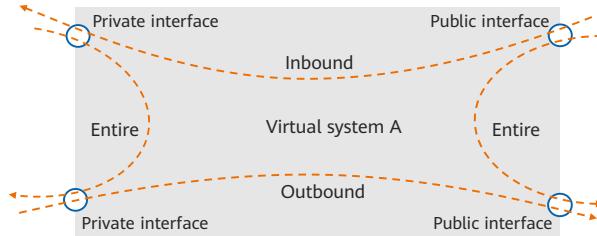


- To manually allocate resources to a virtual system, an administrator needs to configure a resource class, specify the guaranteed number and maximum number of each resource in the resource class, and bind the resource class to the virtual system. The number of resources that a virtual system can use is controlled by the guaranteed and maximum numbers configured in the resource class.
 - Guaranteed number: indicates the minimum number of resources that can be used by a virtual system. Once the minimum number of resources is allocated to the virtual system, the resources are exclusive to the virtual system.
 - Maximum number: indicates the maximum number of resources that can be used by a virtual system. Whether the virtual system can achieve the maximum number depends on the resource usage of other virtual systems.
- If no resource class is bound to a virtual system, the virtual system is not restricted to use resources. The virtual system preempts the available resources of the device with the public system and other virtual systems that have no resource class bound.

- If no maximum or guaranteed number is specified for some resources in the resource class bound to a virtual system, there is no restriction on the use of these resources for the virtual system. The virtual system preempts such resources of the device with the public system and other virtual systems that are not restricted to use the resources.
- Note the following rules when you allocate public IP addresses:
 - In exclusive mode, a public IP address can be allocated only to one virtual system. In free mode, a public IP address can be allocated to multiple virtual systems.
 - The public IP address cannot conflict with the global address of the NAT Server function in the public system.
 - The public IP address cannot conflict with the NAT address pool in the public system.

Manual Allocation — Bandwidth Resource

- Bandwidth resources refer to the bandwidth required by key services on a network. You can manually allocate bandwidth resources to ensure sufficient bandwidth for critical services transmitted over the link when a link is busy.
- Bandwidth resources are classified into inbound bandwidth, outbound bandwidth, and overall bandwidth. The bandwidth limit on a data flow is related to the inbound and outbound interfaces of the flow.



- As shown in the figure, virtual system A has two public interfaces and two private interfaces. The inbound traffic, outbound traffic, and entire traffic of virtual system A are as follows:
 - Inbound traffic: indicates traffic from a public interface to a private interface, which is restricted by the inbound bandwidth.
 - Outbound traffic: indicates traffic from a private interface to a public interface, which is restricted by the outbound bandwidth.
 - Entire traffic: indicates the sum of the inbound traffic, outbound traffic, traffic from a private interface to another private interface, and traffic from a public interface to another public interface, which is restricted by the overall bandwidth.
- The public interface here does not refer to the interface connecting the firewall to the Internet. It is the interface that is configured with the set public-interface command. The private interface is the interface that is not configured with the set public-interface command.
- In inter-virtual system forwarding scenarios, the Virtual-if interface is a public interface by default.

Contents

1. Virtual System Overview
2. **Basic Concepts of Virtual Systems**
 - Independent Virtual System Management
 - Virtual System Resource Allocation
 - **Virtual System Traffic Isolation**
 - Independent Virtual System Configuration
3. Communication Between Virtual Systems
4. Virtual System Configuration

Virtual System Traffic Distribution

- After a packet enters the firewall, the firewall determines the destination virtual system of the packet. If a virtual system is configured on the firewall, the firewall processes the packet based on the policies and entries in the virtual system. If no virtual system is configured on the firewall, the firewall processes the packet based on the policies and entries in the public system.
- Traffic distribution refers to the process of determining the destination virtual system of a packet. The firewall distributes incoming packets to the correct virtual system for processing. The traffic distribution modes are as follows:

Interface-based traffic distribution

When interfaces work at Layer 3, traffic is distributed based on interfaces.

VLAN-based traffic distribution

When interfaces work at Layer 2, traffic is distributed based on VLANs.

VNI-based traffic distribution

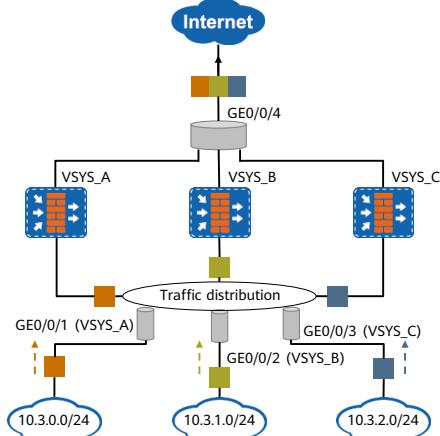
When virtual systems and VXLAN are used together, traffic is distributed based on VNIs.

- VNI-based traffic distribution is not described in this course.

Interface-based Traffic Distribution

- After an interface is bound to a virtual system, all packets received by this interface will be processed by the bound virtual system based on its configuration.
- As shown in the figure, after firewall interfaces are bound to virtual systems according to the following table, packets received by the interfaces will be distributed to the virtual systems bound to the interfaces for routing and policy matching.

Interface	Virtual System
GE0/0/1	VSYS_A
GE0/0/2	VSYS_B
GE0/0/3	VSYS_C

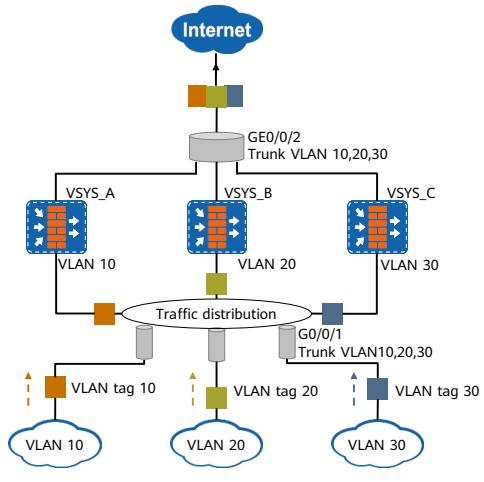


- Note: The management interface GE0/0/0 cannot be allocated to a virtual system as a service interface.

VLAN-based Traffic Distribution

- After a VLAN is bound to a virtual system, packets from this VLAN will be distributed to the bound virtual system for processing.
- As shown in the figure, VLANs are bound to virtual systems according to the following figure. The public system distributes packets from the VLANs to the virtual systems bound to the VLANs. The virtual systems then search their MAC address tables for the outbound interfaces and then forward or discard the packets based on the inter-zone policies.

VLAN	Virtual System
VLAN 10	VSYS_A
VLAN 20	VSYS_B
VLAN 30	VSYS_C



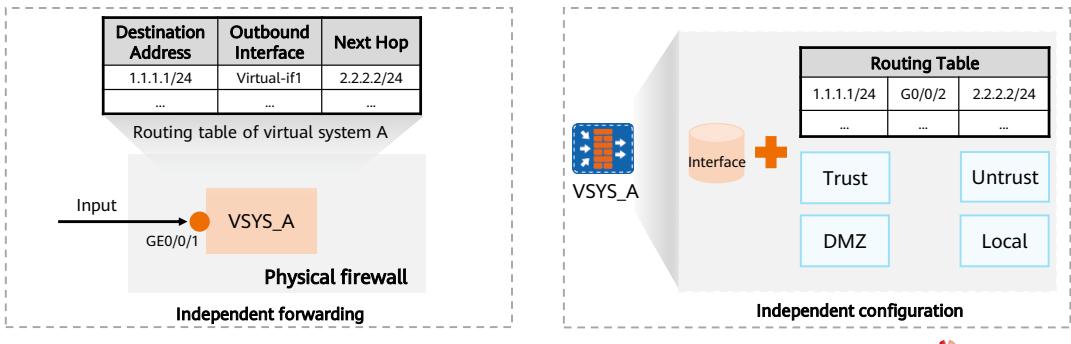
- An interface can transmit traffic from different VLANs, which belong to different virtual systems. Therefore, in VLAN-based traffic distribution, interfaces work at Layer 2 and do not belong to any virtual system.

Contents

1. Virtual System Overview
2. **Basic Concepts of Virtual Systems**
 - Independent Virtual System Management
 - Virtual System Resource Allocation
 - Virtual System Traffic Isolation
 - **Independent Virtual System Configuration**
3. Communication Between Virtual Systems
4. Virtual System Configuration

Independent Virtual System Configuration

- A virtual system has an independent administrator account and an independent configuration page. After a virtual system is bound to an interface on the physical firewall, the traffic received from the interface is forwarded based on the configuration and independent routing entries of the virtual system.
- You can run the **switch vsys vsys-name** command to switch from the system view of the public system to the user view of a specified virtual system.



21 Huawei Confidential



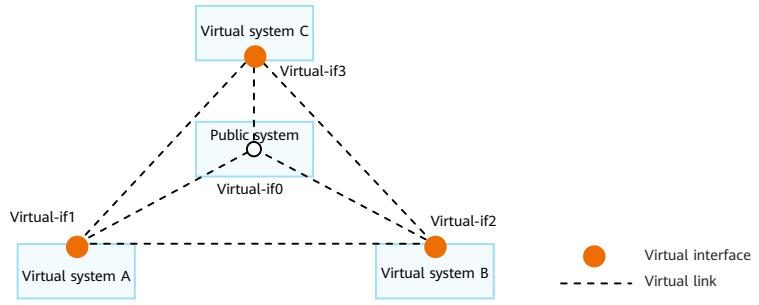
- Virtual systems can also have their own security zones, routing tables, and interfaces.

Contents

1. Virtual System Overview
2. Basic Concepts of Virtual Systems
3. **Communication Between Virtual Systems**
 - Communication Between a Virtual System and the Public System
 - Communication Between Virtual Systems
4. Virtual System Configuration

Virtual Interface

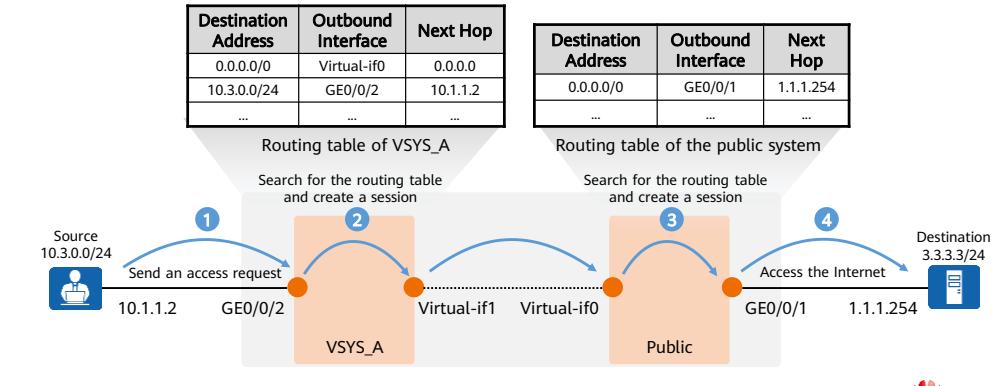
- A virtual interface is a logical interface that is automatically generated for communication with other virtual systems during the creation of a virtual system.
- Virtual interfaces are named in **Virtual-if*number*** format. The virtual interface of the public system is named **Virtual-if0**, while those of other virtual systems are automatically numbered from 1.



- The link status and protocol status of a virtual interface are always up. For communication between virtual systems, each involved virtual interface must be configured with an IP address and added to a security zone in order to operate correctly.
- Virtual interfaces of virtual systems and the public system are connected to form virtual links. As virtual systems and the public system function as independent devices, you can add their virtual interfaces to security zones and configure routes and policies on the virtual interfaces to implement communication between virtual systems and the public system and between virtual systems.

Communication Between a Virtual System and the Public System - Access from a Virtual System to the Public System

- Communication between a virtual system and the public system involves two scenarios: access from the virtual system to the public system and access from the public system to the virtual system. The packet forwarding process differs in the two scenarios. The figure shows the packet forwarding process for a virtual system to access the public system.



24 Huawei Confidential

HUAWEI

- A user in the network segment 10.3.0.0/24 of virtual system A accesses the Internet server at 3.3.3.3 through the public interface GE0/0/1 of the public system. The packet forwarding process is as follows:
 - The client initiates a connection request to the server.
 - After the first packet arrives at the firewall, it is distributed to VSYS_A based on the interface. VSYS_A processes the packet based on the firewall forwarding process, including matching the blacklist, searching for routes, performing NAT, and matching a security policy. If the packet is denied, VSYS_A discards the packet, and the process ends. If the packet is permitted, VSYS_A forwards the packet to the public system. At the same time, VSYS_A creates a session for the connection.
 - After receiving the packet on the virtual interface Virtual-if0, the public system processes the packet based on the firewall forwarding process, including matching the blacklist, searching for routes, performing NAT, and matching a security policy. If the packet is denied, the public system discards the packet, and the process ends. If the packet is permitted, the public system forwards the packet to the server. At the same time, the public system creates a session for the connection.
 - The packet is forwarded to the server according to a route.
 - As both the virtual system and public system need to process the packet based on the firewall forwarding process, policies and routes must be configured for the virtual system and public system.

Route Configuration for a Virtual System to Access the Public System

- Virtual system configuration:

- Configure a forward route, that is, a route to the Internet.

```
[FW-VSYS_A] ip route-static 0.0.0.0 0.0.0.0 public
```

As the packet must be forwarded to the Internet through the public system, the route from the virtual system to the public system is required. It must be a static route. Different from common static routes, this static route does not need to have the next hop or outbound interface specified. Instead, you need to specify the public system as the destination virtual system for the route.

- Configure a return route, that is, a route to the intranet. It can be a dynamic route (such as an OSPF route) or a static route.

```
[FW-VSYS_A] ip route-static 10.3.0.0 255.255.255.0 10.1.1.2
```

- Public system configuration:

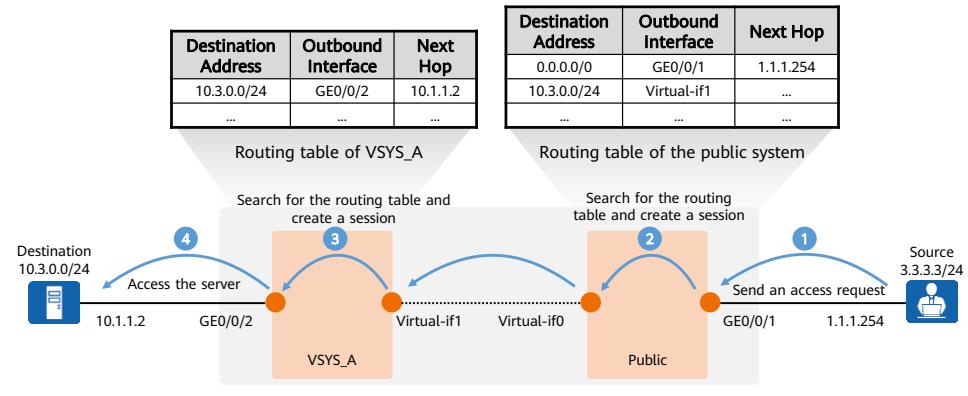
- Configure a forward route, that is, a route to the Internet. It can be a dynamic route (such as an OSPF route) or a static route.

```
[FW] ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
```

Note that you do not need to configure a return route in the public system for the packets replied by the server. After matching a session entry in the public system, the packets replied by the server are directly forwarded to the virtual system. This configuration is different from the route configuration in a virtual system.

Communication Between a Virtual System and the Public System - Access from the Public System to a Virtual System

- As shown in the figure, an Internet user accesses a server attached to the virtual system VSYS_A through the public interface GE0/0/1 of the public system. Packets enter the public system and then the virtual system.



26 Huawei Confidential

HUAWEI

- An Internet user accesses the server attached to VSYS_A through the public interface GE0/0/1 of the public system. The packet forwarding process is as follows:
 - The client initiates a connection request to the server.
 - After receiving the first packet, the public system processes the packet based on the forwarding process, including matching the blacklist, searching for routes, performing NAT, and matching a security policy. If the packet is denied, the public system discards the packet, and the process ends. If the packet is permitted, the public system forwards the packet to VSYS_A through the outbound interface specified in the routing table. At the same time, the public system creates a session for the connection.
 - After receiving the packet on the virtual interface Virtual-if1, the virtual system processes the packet based on the firewall forwarding process, including matching the blacklist, searching for routes, performing NAT, and matching a security policy. If the packet is denied, VSYS_A discards the packet, and the process ends. If the packet is permitted, VSYS_A forwards the packet to the server. At the same time, the virtual system creates a session for the connection.
 - The packet is forwarded to the server according to a route.

Route Configuration for the Public System to Access a Virtual System

- Public system configuration:

- Configure a forward route, that is, a route to the intranet server.

```
[FW] ip route-static 10.3.0.0 255.255.255.0 vpn-instance vsys
```

As the packet must be forwarded to the server through the virtual system, the route from the public system to the virtual system is required. It must be a static route. Different from common static routes, this static route does not need to have the next hop or outbound interface specified. Instead, you need to specify the virtual system attached to the server as the destination virtual system for the route.

- Configure a return route, that is, a route to the Internet. It can be a dynamic route (such as an OSPF route) or a static route.

```
[FW] ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
```

- Virtual system configuration:

- Configure a forward route, that is, a route to the Internet. It can be a dynamic route (such as an OSPF route) or a static route.

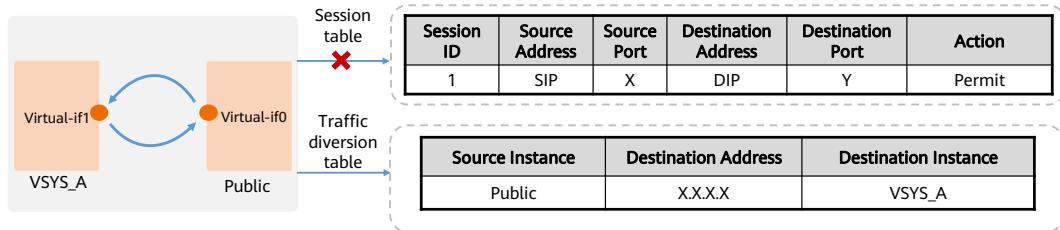
```
[FW-VSYS_A] ip route-static 10.3.0.0 255.255.255.0 10.1.1.2
```

Note that you do not need to configure a return route for the packets replied by the server in the virtual system. After matching a session entry in the virtual system, the packets replied by the server are directly forwarded to the public system. This configuration is different from the route configuration in a virtual system.

- To allow the Internet user to access the server on the intranet, you must configure NAT Server in VSYS_A or the public system to translate addresses.
 - If you configure NAT Server in the public system, the public system translates the destination address of a packet from a public address to a private one before searching the routing table. Therefore, the destination address of the route configured for the public system must be the private address of the server.
 - If you configure NAT Server in the virtual system, the public system forwards the packet to the virtual system, and the virtual system translates the destination address of the packet from a public address to a private one. Therefore, the destination address of the route configured for the public system must be the public address of the server.

Traffic Diversion Table Overview

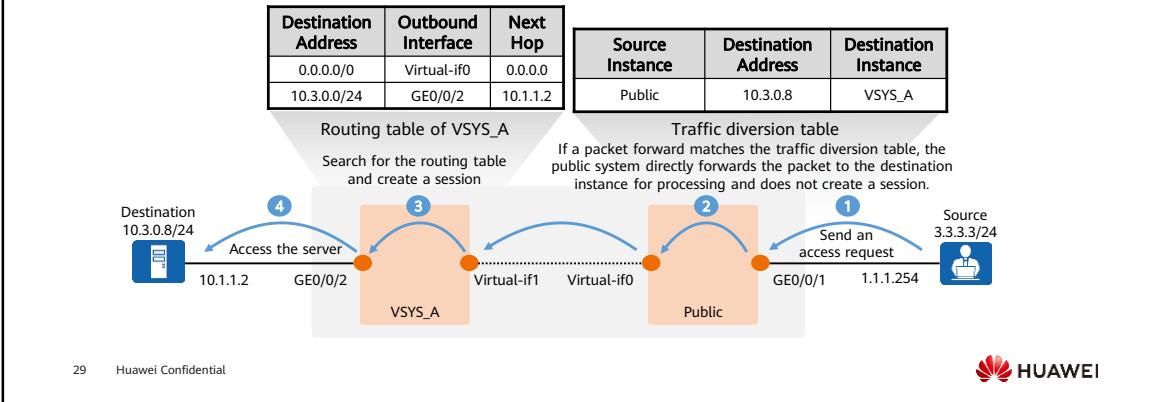
- During communication between a virtual system and the public system, both of them process packets based on the firewall forwarding process. You need to configure policies and create sessions for both the virtual system and public system, which complicates the configuration. Besides, each connection requires two sessions. If the service traffic is heavy, session resources may be insufficient.
- The configured traffic diversion table records the mappings between IP addresses and virtual systems. After matching the traffic diversion table, a packet is directly forwarded by the public system based on the routing table or traffic diversion table without a session being created. This helps solve the preceding problem.



- The traffic diversion table contains the source virtual system, destination address, and destination virtual system.

Traffic Diversion Table - Forward Matching

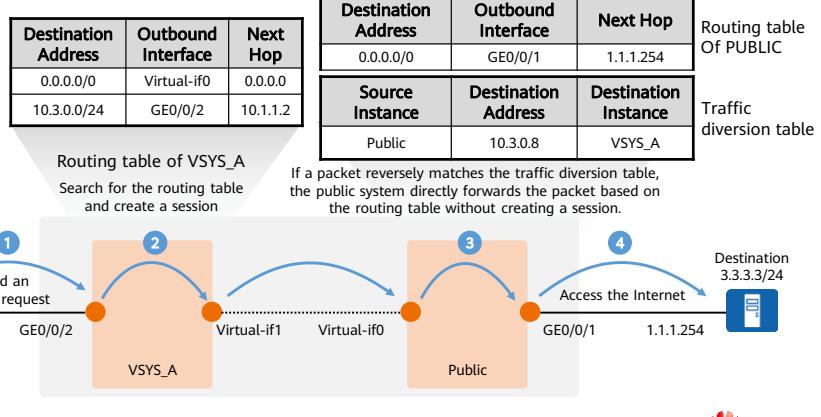
- A packet matches the traffic diversion table in two situations: forward matching and reverse matching.
- Forward matching: The destination address of a packet sent from the public system to a virtual system matches **Destination Address** in the traffic diversion table. In this case, the public system forwards the packet based on the traffic diversion table, that is, sending the packet to **Destination Instance** of the matched entry.



- An Internet user accesses the server attached to VSYS_A through the public interface GE0/0/1 of the public system. The packet forwarding process is as follows:
 - The client initiates a connection request to the server.
 - After the packet arrives at the public system and matches a traffic diversion entry, the public system sends the packet to VSYS_A specified by **Destination Instance** in the matched entry.
 - After receiving the packet on the virtual interface Virtual-if1, the virtual system processes the packet based on the firewall forwarding process, including matching the blacklist, searching for routes, performing NAT, and matching a security policy. If the packet is denied, the virtual system discards the packet, and the process ends. If the packet is permitted, the virtual system forwards the packet to the server. At the same time, the virtual system creates a session for the connection.
 - The packet is forwarded to the server based on a route.

Traffic Diversion Table - Reverse Matching

- Reverse matching: The source address and source virtual system of a packet sent from a virtual system to the public system match **Destination Address** and **Destination Instance** in the traffic diversion table, respectively. In this case, the public system forwards the packet based on the routing table.



30 Huawei Confidential

HUAWEI

- A user in the network segment 10.3.0.0/24 of virtual system A accesses the Internet server at 3.3.3.3 through the public interface GE0/0/1. The packet forwarding process is as follows:
 - The client initiates a connection request to the server.
 - After the first packet arrives at the firewall, the packet is distributed to VSYS_A based on the interface. VSYS_A processes the packet based on the firewall forwarding process, including matching the blacklist, searching for routes, performing NAT, and matching a security policy. If the packet is denied, VSYS_A discards the packet, and the process ends. If the packet is permitted, VSYS_A forwards the packet to the public system. At the same time, VSYS_A creates a session for the connection.
 - After receiving the packet on the virtual interface Virtual-if0, the public system matches the source address of the packet against **Destination Address** in the traffic diversion table. If they match, the public system forwards the packet based on the routing table.
 - The packet is forwarded to the server based on a route.

Contents

1. Virtual System Overview
2. Basic Concepts of Virtual Systems
3. **Communication Between Virtual Systems**
 - Communication Between a Virtual System and the Public System
 - Communication Between Virtual Systems
4. Virtual System Configuration

Communication Between Virtual Systems

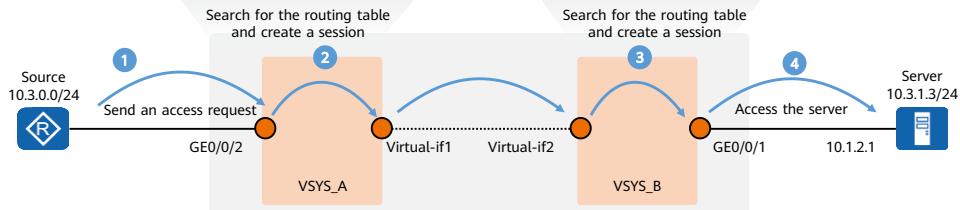
- Virtual systems are isolated by default. As such, hosts attached to different virtual systems cannot communicate with each other. To enable communication between such hosts, you must configure security policies and routes for the virtual systems.

Destination Address	Outbound Interface	Next Hop
10.3.1.3/32	Virtual-if2	0.0.0.0
10.3.0.0/24	GE0/0/2	10.1.1.1
...

Routing table of virtual system A

Destination Address	Outbound Interface	Next Hop
10.3.1.0/24	GE0/0/1	10.1.2.1
...
...

Routing table of virtual system B



- In this scenario, an access request is forwarded from virtual system A to virtual system B. The request packet enters virtual system A, which processes the packet based on the firewall forwarding process. Then, the request packet enters virtual system B, which also processes the packet based on the firewall forwarding process. The detailed process is as follows:
 - The client initiates a connection request to the server.
 - After the first packet arrives at the firewall, traffic is distributed to VSYS_A based on the interface. VSYS_A processes the packet based on the firewall forwarding process, including matching the blacklist, searching for routes, performing NAT, and matching a security policy. If the packet is denied, VSYS_A discards the packet, and the process ends. If the packet is permitted, VSYS_A forwards the packet to VSYS_B. At the same time, VSYS_A creates the following session for the connection.
 - After receiving the packet on the virtual interface Virtual-if2, VSYS_B processes the packet based on the firewall forwarding process, including matching the blacklist, searching for routes, performing NAT, and matching a security policy. If the packet is denied, VSYS_B discards the packet, and the process ends. If the packet is permitted, VSYS_B forwards the packet to the server. At the same time, VSYS_B creates the following session for the connection.
 - The packet is forwarded to the server based on a route.
- As both virtual systems need to process the packet based on the firewall forwarding process, policies and routes must be configured for them.

Route Configuration for Communication Between Virtual Systems

- VSYS_A configuration:

- Configure a forward route, that is, a route to the server.

```
[FW-VSYS_A] ip route-static vpn-instance vsysa 10.3.1.3 255.255.255.0 vpn-instance vsysb
```

As the packet must be forwarded to the server through VSYS_A, the route from VSYS_A to VSYS_B is required. The route between virtual systems can only be a static route. Different from common static routes, this static route does not need to have the next hop or outbound interface specified. Instead, you need to specify the virtual system attached to the server as the destination virtual system for the route.

- Configure a return route, that is, a route to the client. It can be a dynamic route (such as an OSPF route) or a static route. In this example, a static route is configured.

```
[FW-VSYS_A] ip route-static 10.3.0.0 255.255.255.0 10.1.1.1
```

- VSYS_B configuration:

- Configure a forward route, that is, a route to the server. It can be a dynamic route (such as an OSPF route) or a static route. In this example, a static route is configured.

```
[FW-VSYS_B] ip route-static 10.3.1.0 255.255.255.0 10.1.2.1
```

In VSYS_B, you do not need to configure a return route for the packets replied by the server. After matching a session entry in VSYS_B, the packets replied by the server are directly forwarded to VSYS_A.

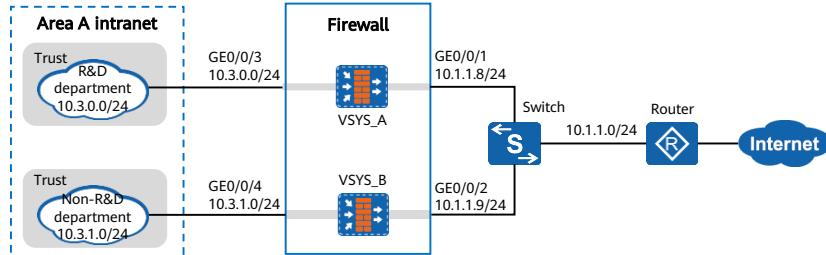
- The preceding configuration allows only the unidirectional communication from VSYS_A to VSYS_B.
- If hosts attached to VSYS_B need to access hosts attached to VSYS_A, you must configure the route from VSYS_B to VSYS_A. For example, if a host attached to VSYS_B accesses a host at 10.3.0.3 attached to VSYS_A, you need to run the **ip route-static vpn-instance vsysb 10.3.0.3 255.255.255.255 vpn-instance vsysa** command to configure a route. In addition, you must configure a policy. The source and destination security zones of the policy are opposite to those when VSYS_A accesses VSYS_B.

Contents

1. Virtual System Overview
2. Basic Concepts of Virtual Systems
3. Communication Between Virtual Systems
- 4. Virtual System Configuration**

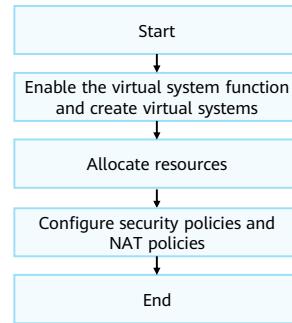
Networking Requirements

- A firewall is deployed in area A of a large campus network as the access gateway. The network of area A comprises the R&D and non-R&D departments, and the two departments have different network access permissions:
 - In the R&D department, only employees on the IP address range from 10.3.0.2 to 10.3.0.10 can access the Internet. In the non-R&D department, all employees can access the Internet.
 - The R&D and non-R&D departments are isolated from each other and cannot communicate.
 - The R&D and non-R&D departments have similar traffic volume. Therefore, the same virtual system resources are allocated to them.



Configuration Roadmap

- Enable the virtual system function.
- The public system administrator creates virtual systems A and B and allocates resources to each virtual system.
- The public system administrator configures IP addresses, routes, security policies, and NAT policies for virtual system A.
- The public system administrator configures IP addresses, routes, security policies, and NAT policies for virtual system B.



Data Planning

VSYS_A information

Virtual System Name	Public Interface/Address	Public Network Security Zone	Private Interface/Address	Private Network Security Zone	Addresses Allowed to Access Public Network
vsysa	GEO/0/1 (10.1.1.8/24)	Untrust	GEO/0/3 (10.3.0.1/24)	Trust	10.3.0.2/24-10.3.0.10/24

VSYS_B information

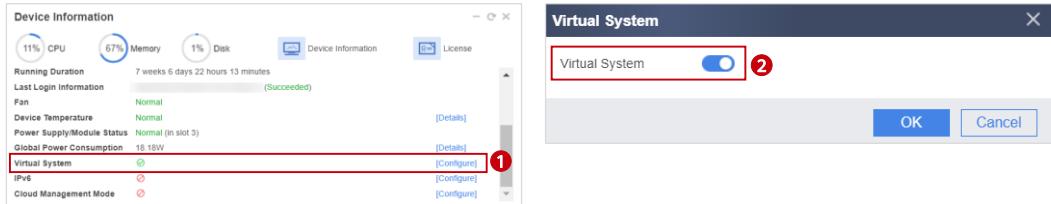
Virtual System Name	Public Interface/Address	Public Network Security Zone	Private Interface/Address	Private Network Security Zone	Private Network Address Range
vsysb	GEO/0/2 (10.1.1.9/24)	Untrust	GEO/0/4 (10.3.1.1/24)	Trust	10.3.1.0/24

Resource class information

Name	Guaranteed/Maximum Number of Sessions	User Quantity	User Group	Policy Quantity	Outbound Bandwidth
r1	10000/50000	300	10	300	20 M

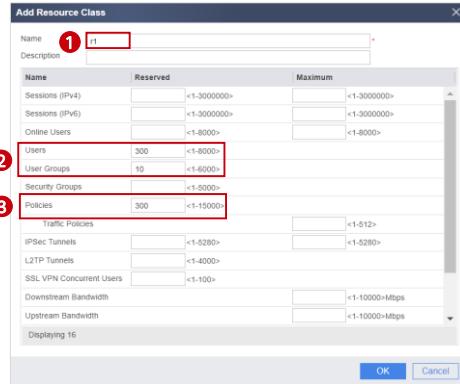
Enabling the Virtual System Function

- Choose **Dashboard > Device Information**. Click **Configure** next to **Virtual System** to enable the virtual system function.



Configuring a Resource Class

- Choose **System > Virtual System > Resource Class**. Click **Add** and set the resource class name, guaranteed number and maximum number of sessions, number of users, number of user groups, number of policies, and overall bandwidth as follows.



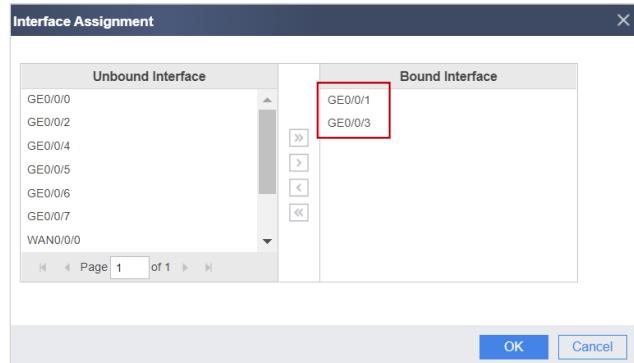
Creating a Virtual System and Allocating a Resource Class

- Choose **System > Virtual System > Virtual System**. Click **Add**. In the dialog box displayed, click the **Basic Settings** tab, set the virtual system name, set the resource class to **r1**, and click **OK**.



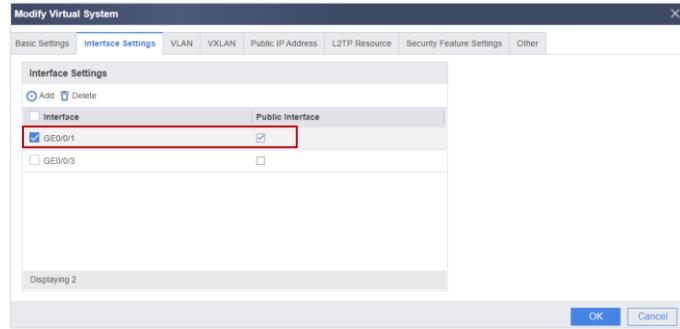
Allocating Interfaces

- Click the **Interface Settings** tab, allocate GE0/0/1 and GE0/0/3 to virtual system A, and click **OK**.



Setting the Public Interface

- Configure GE0/0/1 as the public interface. Bandwidth resource configurations in the resource class take effect only after the public interface is configured.
- Repeat the preceding steps to create virtual system B, allocate resource class r1 and interfaces GE0/0/2 and GE0/0/4 to it, and configure GE0/0/2 as the public interface. The configuration procedure of virtual system B is similar to that of virtual system A and is not described here.



Configuring IP Addresses

- Set interface parameters in virtual system A.
 - Select **vysa** from the **Virtual System** drop-down list in the upper right corner to access virtual system A.

The screenshot shows two side-by-side interface configuration windows for virtual system A. Both windows have a header with 'admin' (dropdown), 'Commit', 'Save', and a three-dot menu. The left window is titled 'Modify GigabitEthernet Interface' and shows settings for 'GigabitEthernet0/0/1'. It has fields for 'Interface Name', 'Alias' (empty), 'Virtual System' (dropdown set to 'vysa'), 'Zone' (dropdown set to 'untrust' with 'Routing' selected), and 'Mode' (radio buttons for 'Routing', 'Switching', 'Bypass', and 'Interface Pair'). Under the 'IPv4' tab, the 'IP Address' field contains '10.1.1.8/24' (marked with red box 2). The right window is also titled 'Modify GigabitEthernet Interface' and shows settings for 'GigabitEthernet0/0/3'. It has similar fields: 'Interface Name' (GigabitEthernet0/0/3), 'Virtual System' (dropdown set to 'vysa'), 'Zone' (dropdown set to 'trust' with 'Routing' selected), and 'Mode' (radio buttons for 'Routing', 'Switching', 'Bypass', and 'Interface Pair'). Under the 'IPv4' tab, the 'IP Address' field contains '10.3.0.1/255.255.255.0' (marked with red box 4). Both windows have a note below the IP address input field: 'Enter each IP address on a separate line.' followed by examples: '10.50.1.2/255.255.255.0' and '10.10.1.2/24'.

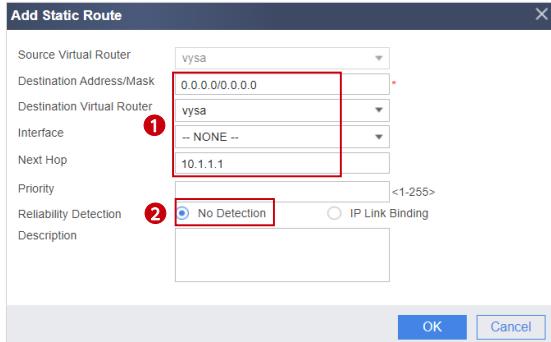
43 Huawei Confidential



- Repeat the preceding steps to set interface parameters for virtual system B.

Configuring a Route

- Configure a route in virtual system A to enable it to access the Internet.
 - Choose **Network > Route > Static Route**.
 - Click **Add** and configure a default static route from virtual system A to the Internet. The parameter settings are as follows.



44 Huawei Confidential

 HUAWEI

Configuring a Security Policy

- Configure a security policy in virtual system A to allow R&D employees on a specific network segment to access the Internet.
 - Choose **Object > Address**.
 - Click **Add** and create an IP address range shown in the upper right figure.
 - Choose **Policy > Security Policy > Security Policy**.
 - Choose **Add > Add Security Policy** and configure a security policy to allow ipaddress1 to access the Internet.

The figure consists of two screenshots of the Huawei USG firewall configuration interface. The top screenshot shows the 'Add Address' dialog. It has fields for Name (ipaddress1), Description, Address Group (selected), and IP Address/Rage or MAC Address (19.3.0.2-19.3.0.10). The bottom screenshot shows the 'Add Security Policy' dialog. It has sections for General Settings (Name: to_internet, Policy Group: NONE, Tag: selected), Source and Destination (Source Zone: trust, Destination Zone: untrust, Source Address/Region: ipaddress1), User and Service (User: selected, Service: selected, Application: selected), and Action (Action: Permit). Red boxes and numbers 1, 2, and 3 highlight specific fields: 1 highlights the 'ipaddress1' entry in the address/range field; 2 highlights the 'ipaddress1' entry in the source address field; 3 highlights the 'Permit' radio button in the action section.

45 Huawei Confidential



- Packets from employees on other network segments to the Internet will match the default security policy and are denied.

Configuring a NAT Policy

- Configure a NAT policy in virtual system A. Choose **Policy > NAT Policy > NAT Policy**, click **Add**, and configure a NAT policy as follows.

The screenshot shows the 'Add NAT Policy' configuration page. The 'Original Data Packet' section includes fields for Source Zone (set to 'trust'), Destination Type (set to 'Destination Zone'), Source Address (set to 'GE0/0/1'), and Destination Address (set to 'ipaddress1'). The 'Translated Data Packet' section includes a field for 'Source Address Translated To' (set to 'Address in the IP address'). The 'Outbound Interface' field is highlighted with a red box and contains the value 'GE0/0/2'. The 'Outbound interface' checkbox is also highlighted with a red box. Numbered callouts point to specific fields: ① points to the NAT type selection (NAT), ② points to the Source Zone ('trust'), ③ points to the Outbound Interface field ('GE0/0/2'), ④ points to the Destination Address ('ipaddress1'), and ⑤ points to the Outbound interface checkbox.

46 Huawei Confidential



- The public system administrator configures IP addresses, routes, security policies, and NAT policies for virtual system B. The configuration is similar to that of the R&D department except the following:
 - The IP address of the public interface is different.
 - You do not need to create an IP address range for the non-R&D department. You only need to configure a security policy to allow all IP addresses to access the Internet and another security policy to allow employee communication.
 - The outbound interface of the NAT policy is GE0/0/2, and the source address is any.

Quiz

1. (True or false) The management interface of the firewall cannot be allocated to a virtual system. ()
 - A. True
 - B. False
2. (Multiple-answer question) Which of the following traffic distribution modes are supported by virtual systems? ()
 - A. Interface-based traffic distribution
 - B. VLAN-based traffic distribution
 - C. VNI-based traffic distribution
 - D. Protocol-based traffic distribution

1. A
2. ABC

Summary

- This course describes the basic concepts of virtual systems, how virtual systems implement service and route isolation, route configurations in different application scenarios. Virtual systems can be configured to isolate services in multiple scenarios, reducing hardware costs and O&M pressure of administrators.
- Upon completion of this course, you will be able to understand the basic concepts of virtual systems and independently configure virtual systems.

Recommendations

- Huawei official websites
 - Enterprise service: <https://e.huawei.com/en/>
 - Technical support: <https://support.huawei.com/enterprise/en/index.html>
 - Online learning: <https://learning.huawei.com/en/>

Acronyms and Abbreviations

Acronym/Abbreviation	Full Name
DMZ	Demilitarized Zone
CPU	Central Processing Unit
I/O	Input/Output
NAT	Network Address Translation
OSPF	Open Shortest Path First
SSL	Secure Sockets Layer
VLAN	Virtual Local Area Network
VNI	VXLAN Network Identifier
VPN	Virtual Private Network
VSYS	Virtual System
VXLAN	Virtual Extensible Local Area Network

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。
Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

Copyright©2022 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product performance, market position, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.



Firewall Intelligent Uplink Selection



Foreword

- In the actual networking, an enterprise usually leases multiple carrier links to meet bandwidth and reliability requirements. This prevents risks due to the single link failure and provides more bandwidth resources. When forwarding traffic, the egress device randomly selects a link without considering the actual bandwidth or real-time status of each link. As a result, new problems such as link idleness or congestion occur.
- Intelligent uplink selection can be deployed on egress firewalls to solve the preceding problems. The firewall uses different intelligent uplink selection modes to dynamically select the optimal link, improving link resource utilization and user experience.
- This course describes the principles and applications of intelligent uplink selection.

Objectives

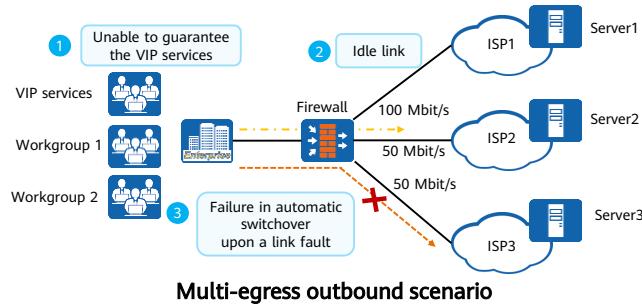
- On completion of this course, you will be able to:
 - Describe basic concepts of intelligent uplink selection.
 - Describe the application scenarios of intelligent uplink selection.
 - Master the configuration procedure of intelligent uplink selection.

Contents

- 1. Overview of Intelligent Uplink Selection**
2. Principles of Intelligent Uplink Selection
3. Configuration of Intelligent Uplink Selection

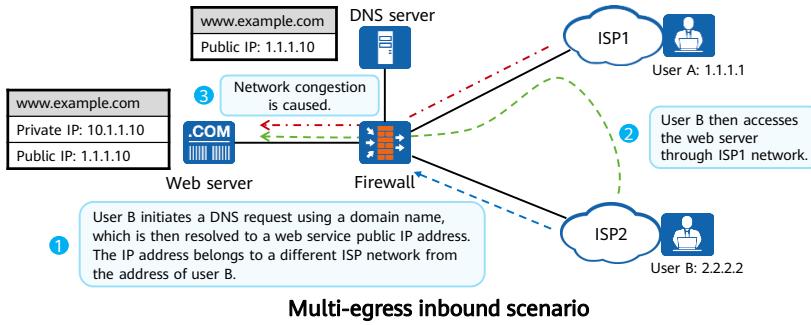
Background of Intelligent Uplink Selection (1/2)

- Medium- and large-sized enterprises usually deploy multiple links at the network egress to improve egress link bandwidth and reliability. In multi-egress scenarios, the traditional method is using equal-cost routes. However, equal-cost routes cause a large number of cross-ISP access requests, resulting in low access efficiency. In addition, the firewall does not consider the actual bandwidth or real-time status of each link when forwarding packets. In practical applications, problems such as link congestion and poor user experience may occur.



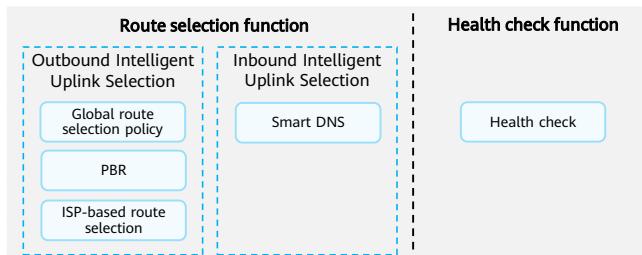
Background of Intelligent Uplink Selection (2/2)

- Assume that both DNS and web servers are deployed on the enterprise intranet. When an Internet user accesses the web server on the enterprise intranet using a domain name, the address after DNS resolution may belong to a different ISP network from the user address. As a result, access latency, extra inter-ISPs traffic costs, or link congestion may occur.



Overview of Intelligent Uplink Selection

- When there are multiple links to the destination network, the firewall uses different intelligent uplink selection modes to dynamically select the optimal link and dynamically adjusts the allocation result based on the real-time status of each link, improving link resource utilization and user experience.
- Intelligent uplink selection provides the following functions:
 - Route selection: To meet the requirements of multiple scenarios, the route selection function corresponds to different intelligent uplink selection technologies based on inbound and outbound scenarios.
 - Health check: This function can probe the service or link availability or the link latency and adjust traffic distribution based on probe results to guarantee service quality.



6 Huawei Confidential

 HUAWEI

- Outbound and inbound intelligent uplink selection methods are implemented in different ways:
 - Outbound intelligent uplink selection: When an intranet user accesses the Internet, the firewall performs intelligent uplink selection if there are multiple links to the destination network.
 - Global route selection policy: When there are multiple equal-cost routes or default routes to the destination network, the firewall dynamically selects the optimal link based on different intelligent uplink selection modes.
 - Policy-based routing (PBR): When PBR is configured on the network and traffic matches the configured PBR, the firewall dynamically selects the optimal link based on different intelligent uplink selection modes if there are multiple links to the destination network.
 - ISP route selection: When the firewall functions as an egress gateway that connects to multiple ISP networks, it generates ISP routes in batches so that traffic destined for a specific ISP network is forwarded through the corresponding outbound interface. This ensures that traffic is forwarded along the shortest path.

- Inbound intelligent uplink selection: When an Internet user accesses the intranet, the firewall performs intelligent uplink selection if there are multiple links to the destination network.
 - Smart DNS: When an Internet user accesses an intranet server using a domain name, the user sends a DNS request to the intranet DNS server, which returns the resolved address to the Internet user. In this process, the firewall intelligently changes the resolved address in the DNS response packet so that the user can obtain the most appropriate resolved address, preventing link congestion or cross-ISP access.
- Generally, health check is not used independently. It takes effect only when it is used together with intelligent uplink selection. Currently, the health check function can be used only with the outbound intelligent uplink selection function.

Contents

1. Overview of Intelligent Uplink Selection
2. **Principles of Intelligent Uplink Selection**
 - Outbound Intelligent Uplink Selection
 - Inbound Intelligent Uplink Selection
 - Health Check
3. Configuration of Intelligent Uplink Selection

Outbound Intelligent Uplink Selection - Global Route Selection Policy

- In a multi-egress scenario, the global route selection policy can select outbound interfaces based on different intelligent uplink selection modes and dynamically adjust the allocation result based on the real-time status of each link, thereby improving link resource utilization and user experience.
- You can also set an overload protection threshold for a link as required. When the traffic carried by a link exceeds the threshold, overload protection load-balances the excess traffic among the links that do not exceed the threshold.

Intelligent Uplink Selection Mode

Load balancing by link bandwidth

- The firewall distributes traffic to each link based on the bandwidth ratio.

Load balancing by link quality

- The firewall preferentially uses the link with the highest quality to forward traffic.

Load balancing by link weight

- The firewall distributes traffic to each link based on the weight ratio.

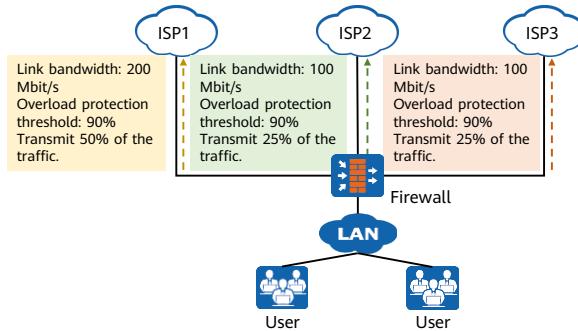
Active/standby backup by link priority

- The firewall preferentially uses the main interface to forward traffic.

- In the multi-egress scenario where equal-cost routes exist, the firewall forwards packets in per-flow load balancing mode by default. The firewall uses the source and destination IP addresses to perform hash calculation to select an outbound interface. That is, the route is determined based on the source and destination IP addresses of packets, without considering the actual bandwidth or real-time status of each link. If the traffic volume is large, some links may be congested and the others may be idle, which causes a waste of link resources. When a link has poor transmission quality, Internet access through this link may fail, which compromises user experience.

Global Route Selection Policy - Load Balancing by Link Bandwidth

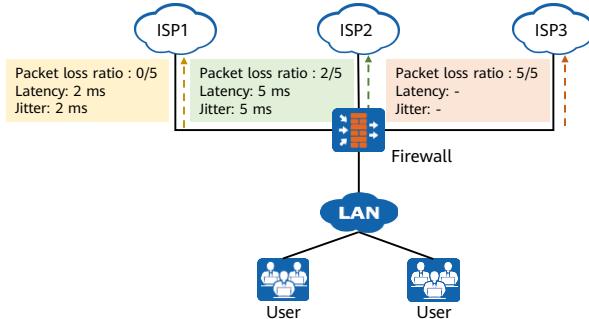
- When an enterprise obtains multiple links with different bandwidths from different ISPs, you can select the link bandwidth-based load balancing mode to fully utilize the bandwidth of each link. This mode is also the default intelligent uplink selection mode.
- When deploying a firewall, you need to configure the inbound and outbound bandwidths on the outbound interface of each link based on the actual link bandwidth.



- As shown in the figure, the firewall has three links connected to outbound interfaces. The bandwidth of the link connected to ISP1 is 200 Mbit/s, and the bandwidth of the links connected to ISP2 and ISP3 is 100 Mbit/s. Therefore, the bandwidth ratio is 2:1:1. After the firewall has forwarded traffic for a while, the traffic statistics show that the history traffic of each link accounts for 50%, 25%, and 25% of the total traffic. That is, the ratio of traffic on each link is in proportion with the bandwidth ratio.
- To ensure that the links are not overloaded, you can set an overload protection threshold for each link (90% for all links). If the bandwidth usage of a link reaches 90%, traffic for existing sessions is still forwarded over the link, and traffic for new sessions will not be forwarded over the link. The firewall will implement load balancing based on the bandwidth ratio of unloaded links for traffic of new sessions. When all links are overloaded, the firewall continues to forward traffic based on the bandwidth ratio of all links.

Global Route Selection Policy - Load Balancing by Link Quality

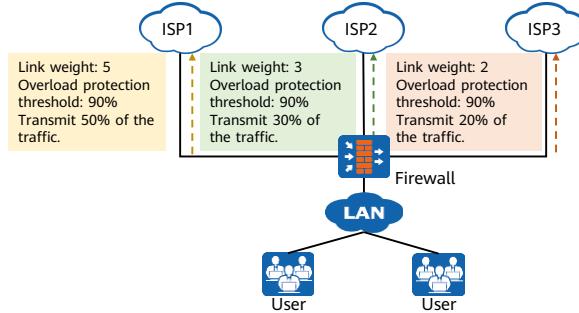
- If an enterprise has multiple ISP links and the firewall needs to dynamically adjust traffic forwarding based on real-time traffic transmission quality of each link, you can set the route selection mode to load balancing by link quality.
- The packet loss ratio, latency, and jitter are three parameters used by the firewall to measure link quality. You can select one or more parameters as required to determine link quality.



- As shown in the figure, the firewall has three links connected to outbound interfaces that belong to different ISPs. The firewall sends five probe packets to the specified device on each ISP network. No packet is dropped on ISP1 link, two packets are dropped on ISP2 link, and ISP3 link does not have any response packets. Therefore, the firewall determines that ISP1 link has the highest quality and uses ISP1 link preferentially to forward traffic, as long as the probe entry is not aged out.
- If you set an overload protection threshold for each link and the bandwidth utilization of ISP1 link reaches the threshold, ISP1 link is excluded from intelligent uplink selection. In this case, the firewall uses the link with the second highest quality (ISP2 link) to forward subsequent traffic.
- Among the three parameters, the packet loss ratio is the most important. If the packet loss ratio, latency, and jitter of two links are different, the firewall considers the link with a smaller packet loss ratio has the higher quality link.

Global Route Selection Policy - Load Balancing by Link Weight

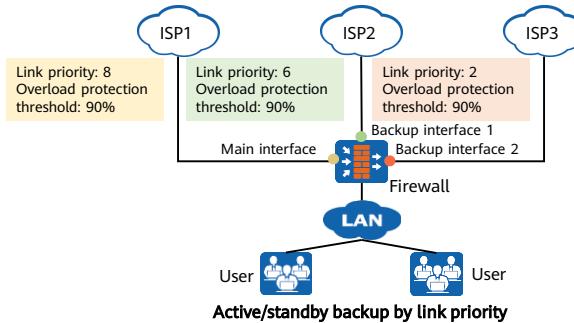
- If an enterprise has ISP links with different performance, the link with the best performance can be selected to ensure the experience of most users and maximize the efficiency of other links. In such scenarios, the link selection mode can be set to load balancing by link weight.
- When specifying the weight for each interface on the firewall, the administrator needs to consider the bandwidth, forwarding latency, and link lease expense of each link.



- As shown in the figure, the firewall has three links connected to outbound interfaces that belong to different ISPs. The weights of ISP1, ISP2, and ISP3 links are respectively 5, 3, and 2. The weight ratio is 5:3:2. After the firewall has forwarded traffic for a while, the traffic statistics show that the history traffic of each link accounts for 50%, 30%, and 20% of the total traffic. That is, the ratio of traffic on each link is in proportion with the weight ratio.
- To ensure that the links are not overloaded, you can set an overload protection threshold for each link (90% for all links). When the bandwidth utilization of a link reaches 90%, the firewall no longer forwards traffic to this link and implements load balancing based on the weight ratio of the links that are not overloaded. When all links are overloaded, the firewall continues to forward traffic based on the weight ratio of all links.
- The link with the optimal forwarding performance refers to the link that meets the enterprise's interests best, not the link with the fastest forwarding speed. Therefore, you need to set a proper weight based on the actual situation.

Global Route Selection Policy - Active/Standy Backup by Link Priority

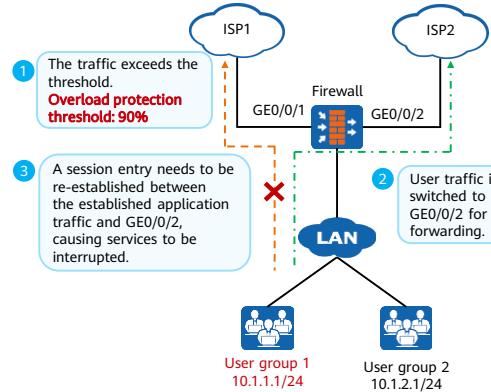
- When an enterprise obtains multiple links from different ISPs and the bandwidth and forwarding latency of the links vary greatly, you can increase the priorities of some links to make the interfaces on these links main interfaces for preferentially transmitting traffic; and other links function as backup links or load balancing links. This mode is an active/standby backup by link priority, which includes active/standby backup and load balancing.



- This intelligent uplink selection mode applies to the following scenarios:
 - Active/standby backup scenario: The firewall preferentially uses the main interface to forward traffic. If no overload protection threshold is specified for the main interface, the firewall will not use other links to transmit traffic even if the link is overloaded. The backup interface with the second highest priority is activated to substitute the main interface only after the link of the main interface fails. Other backup interfaces with lower priorities remain backup.
 - Load balancing scenario: To improve transmission reliability and load capability, set an overload protection threshold for each interface link. When the main interface is overloaded, the firewall will use the backup interface with the second highest priority to share the traffic load with the main interface. If both the main interface and the backup interface with the highest priority are overloaded, the interface with the highest priority among the other backup interfaces is activated to forward traffic.
- As shown in the figure, the firewall has three links connected to outbound interfaces that belong to different ISPs. The priorities of ISP1, ISP2, and ISP3 links are 8, 6, and 2, respectively. ISP1 link has the highest priority. The firewall preferentially uses ISP1 link to forward traffic.
- In the figure above, the administrator sets the overload protection threshold of 90% for each link. The firewall uses ISP1 link preferentially to forward traffic. When the bandwidth utilization of ISP1 link reaches 90%, ISP2 link is activated to share the traffic load with ISP1 link. When both ISP1 and ISP2 links are overloaded, ISP3 link is activated to share the traffic load with ISP1 and ISP2 links. If the three links are all overloaded, the firewall will forward traffic to the three links by bandwidth ratio, not by link priority.

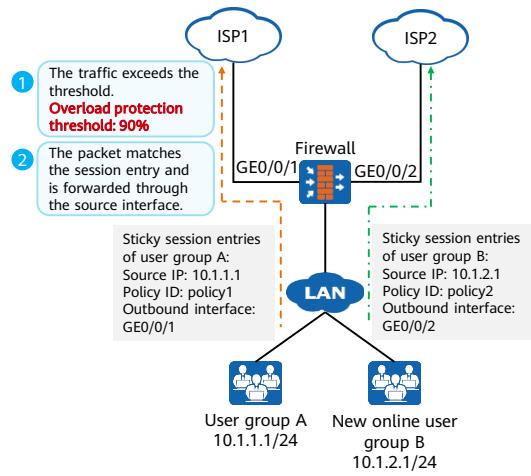
Problems of Overload Protection

- You can configure an overload protection threshold for each intelligent uplink selection interface. When the bandwidth utilization of an interface link reaches the overload protection threshold, the firewall excludes the overloaded link when selecting routes for new traffic.
- The Internet access traffic of some users may have selected the link before it is overloaded, but the new session traffic (such as opening a new web page) is forwarded by another interface on the firewall after the link is overloaded. In this case, the following phenomena may occur: Users need to re-log in after the accessed web pages are refreshed; online games are disconnected; and even some online banking services deny user access due to an IP address change detected.



Sticky Session

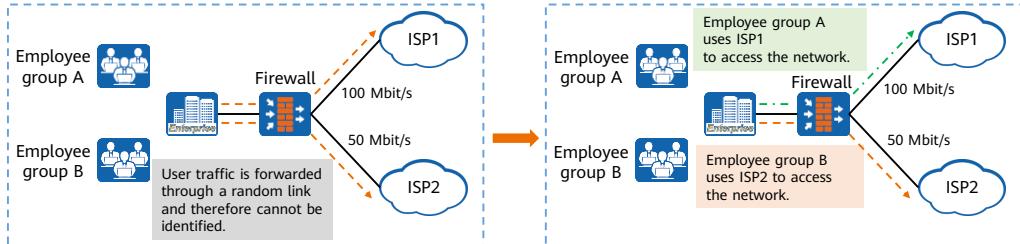
- To resolve the problems facing overload protection, enable the sticky session function for intelligent uplink selection. After intelligent uplink selection is performed for the Internet access traffic of user A for the first time, a sticky session entry is generated. The sticky session entry contains the source IP address, matched intelligent uplink selection policy ID, and outbound interface for the first route selection. When user A initiates connections again, the firewall will look up the sticky session entry based on the traffic source IP address and matched intelligent uplink selection policy ID and forwards the traffic from the outbound interface recorded in the sticky session entry. In this way, the traffic of user A is always forwarded from the same outbound interface. For new online intranet users, another interface is selected and sticky session entries are generated for them.
- You can run the **display session persistence table** command to view sticky session entries.



- Huawei USG6000E series supports the sticky session function in four intelligent uplink selection modes.

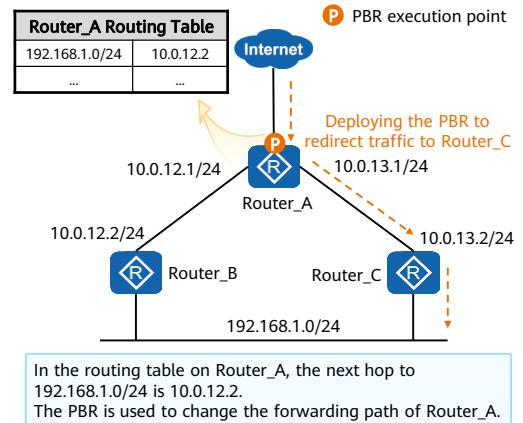
Outbound Intelligent Uplink Selection – PBR

- The global route selection policy selects routes based on link impact parameters and cannot provide differentiated services. If you specify a path to forward traffic, you can use PBR to select a path. PBR takes precedence over a routing table. With PBR, policies can be formulated based on more dimensions (such as inbound interface, source security zone, source/destination IP address, user, service, and application) to determine packet forwarding paths, improving flexibility in packet forwarding control.
- As shown in the figure, in the dual ISP access scenario, employee group A of an enterprise has high permissions and needs to access the Internet through link ISP1 (100 Mbit/s); employee group B has low permissions and needs to access the Internet through link ISP2 (50 Mbit/s). This requirement cannot be implemented using traditional routing technologies, but can be implemented using PBR.



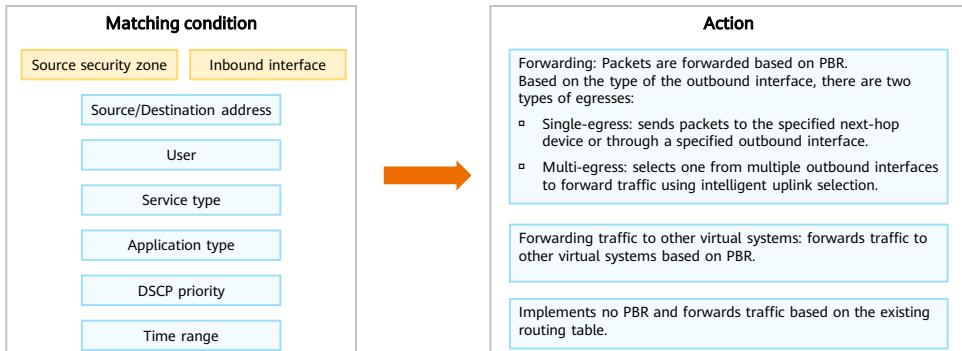
Basic Concepts of PBR

- PBR enables a network device to forward data not only based on the destination IP address of a packet, but also based on other elements, such as the source IP address, source and destination MAC addresses, and source and destination port numbers.
- You can also use an ACL to match specific packets, and then implement PBR based on the ACL.
- If PBR is deployed on a device, matched packets are preferentially forwarded based on the PBR policy. That is, the PBR policy has a higher priority than the traditional routing table.



PBR Matching Rules (1/2)

- PBR consists of multiple nodes, each consisting of matching conditions and an action.
 - Matching conditions can be used to identify traffic for which PBR is to be performed. The source security zone and inbound interface are mutually exclusive. Either of them must be configured.
 - If the traffic matches all the matching conditions of the PBR rule, the traffic matches the PBR rule and the action of the PBR rule is performed.



- You can specify multiple services or service groups, applications or application groups, and users or user groups. The traffic matches the matching conditions as long as it matches any specified service, application, and user.

PBR Matching Rules (2/2)

- After receiving traffic, the firewall identifies the traffic attributes and matches the traffic attributes with the matching conditions of a PBR rule. If all conditions are matched, the traffic matches the PBR rule. After the traffic matches the PBR rule, the device performs the action defined in the PBR rule.
- A PBR rule contains multiple matching conditions, which are ANDed. A packet matches the rule only when it matches all the conditions of the rule.
- Multiple PBR policies are ORed. The device matches traffic against PBR policies one by one from the top of the policy list until a matched PBR policy is found.

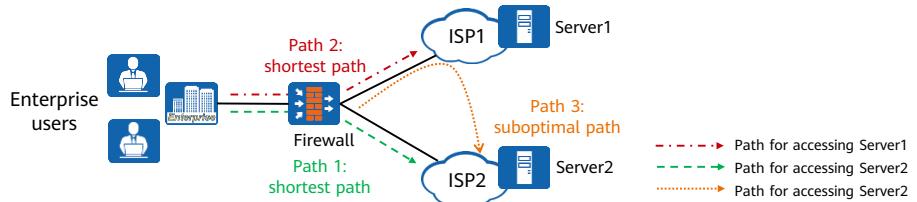


Policy ID	Matching Condition				Action
Policy 1:	Matching condition 1	Matching condition 2	...	Matching condition N	Action
Policy 2:	Matching condition 1	Matching condition 2	...	Matching condition N	Action
			...		
Policy N:	Matching condition 1	Matching condition 2	...	Matching condition N	Action
Default:	Any				Action (No PBR)

- PBR rules are sorted in the configuration sequence by default. An earlier configured PBR rule has a higher priority. The device matches traffic against PBR policies one by one from the top of the policy list until a matched PBR policy is found. As such, the sequence of configuring PBR policies is important. You need to configure policies with the more specific conditions before those with general conditions. If a specific PBR policy is placed after a general PBR policy, the specific PBR policy may never be matched.
- In addition, the system has a default PBR policy **default**, which is at the bottom of the policy list and has the lowest priority. All matching conditions are **Any**, and the action is **No PBR**. That is, packets are forwarded based on the existing routing table. If none of the configured policies is matched, the default PBR policy **default** is matched.

Outbound Intelligent Uplink Selection - ISP-based Route Selection

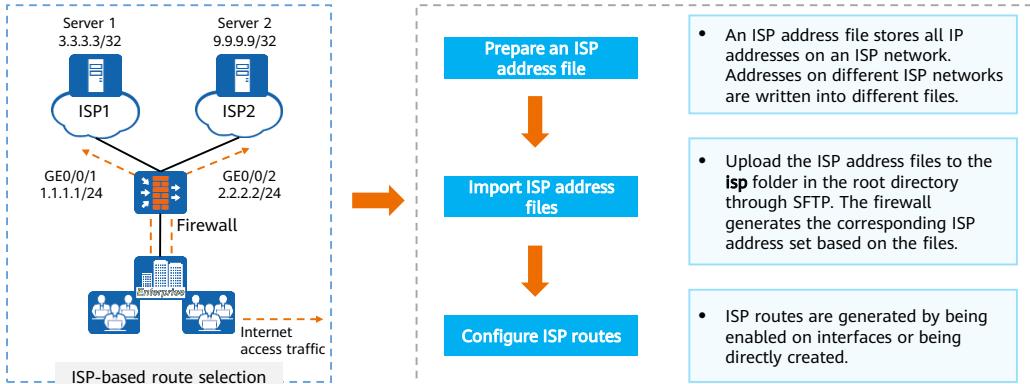
- ISP-based route selection is also called ISP address library-based link selection. When the firewall functions as an egress gateway and connects to multiple ISP networks, you can enable ISP-based route selection on the firewall to forward the traffic to a specific ISP network from the corresponding outbound interface. This ensures that the traffic is forwarded on the shortest path.
- Assume that ISP-based route selection has been configured. In this case, when an intranet user accesses Server1 or Server2, the firewall selects an outbound interface based on the ISP network where the destination address resides to enable the access traffic to reach Server1 through the shortest path, avoiding suboptimal paths.



- As shown in the following figure, the firewall has two ISP links to the Internet. When an intranet user accesses the Server2 on the ISP2 network, the firewall can reach the Server2 through multiple paths if equal-cost routes exist on the firewall. Apparently, path 3 is not the best path, and path 1 is the most desired path.

Implementation of ISP-based Route Selection on the Firewall

- ISP-based route selection is based on ISP routes. Routes are generated in batches based on the imported ISP addresses. In this way, packets destined for a specific ISP network are forwarded through the corresponding outbound interface. ISP-based route selection can be used independently or together with other intelligent uplink selection functions.



- As shown in the figure, the firewall is deployed at the network egress as a security gateway. The enterprise has two links connected to ISP1 and ISP2, respectively.
 - Requirements:**
 - The enterprise requires that packets to Server 1 and Server 2 be forwarded on the links connected to ISP1 and ISP2, respectively.
 - When one link is faulty, follow-up traffic will be forwarded on the other link to ensure transmission availability.
 - Workflow:**
 - Configure health check for ISP1 and ISP2 links to detect the link status.
 - Make two ISP address files, **isp1.csv** and **isp2.csv**, write Server 1 IP address 3.3.3.3/32 into **isp1.csv** and Server 2 IP address 9.9.9.9/32 into **isp2.csv**, and upload the two ISP address files to the firewall.
 - Configure ISP-based route selection to forward packets destined for Server 1 from ISP1 link and packets destined for Server 2 link from ISP2 link.
 - Configure a basic security policy to allow intranet users to access the Internet.
- Currently, the ISP address file can be obtained in either of the following ways:
 - Method 1:** Log in to Huawei Security Center (isecurity.huawei.com) and choose **Signature Update**. Select the corresponding model and version, switch to the Internet Service Provider tab page, and download the latest ISP address file. You can modify the file based on the site requirements.

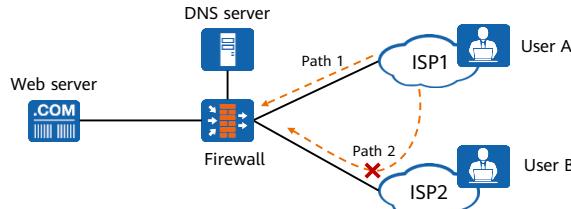
- Method 2: On the web configuration page of the firewall , click **Add Carrier** to download the ISP address file template and edit it locally.
- Import the ISP address file:
 - You can upload the ISP address file to the firewall through SFTP or on the web UI. The imported ISP address file is stored in the **isp** folder in the root directory.
- You can configure ISP routes in either of the following methods:
 - Method 1: Enable ISP routes on interfaces: Specify an ISP address set on an interface to generate ISP routes. Only one ISP address set can be specified for an interface.
 - Method 2: Create ISP routes directly: Create ISP routes directly. You can specify multiple ISP address sets for the same interface.
- The ISP address files of the following carriers are preset on the firewall before delivery: china-mobile.csv (China Mobile), china-unicom.csv (China Unicom), china-telecom.csv (China Telecom), and china-educationnet.csv (CERNET).
- Precautions for the ISP address file:
 - The file must be in CSV format.
 - You can use the predefined ISP address file on the firewall directly or change the file if necessary.
 - The predefined and imported ISP address files are stored in the **isp** folder in the root directory. After you import ISP address files, you need to create a name for each file. Usually, it is usually named after the carrier represented by the ISP. Each ISP address file will automatically generate an ISP address group (also called a carrier address group) after being imported. The ISP address group contains all IP addresses in the ISP address file. You can reference the address group as the source or destination address in PBR policies.
- The protocol type of ISP routes displayed in the routing table is User Network Route (UNR), and the route priority is 70.
- To improve traffic forwarding reliability, ISP-based route selection can function with health check to prevent traffic from being forwarded over a faulty link. If the health check result indicates that a link is faulty, the corresponding ISP route entry will be deleted. Therefore, traffic will not match this route. After the link recovers, the ISP route entry is regenerated, and traffic can be forwarded over this route.

Contents

1. Overview of Intelligent Uplink Selection
2. **Principles of Intelligent Uplink Selection**
 - Outbound Intelligent Uplink Selection
 - **Inbound Intelligent Uplink Selection**
 - Health Check
3. Configuration of Intelligent Uplink Selection

Inbound Intelligent Uplink Selection - Smart DNS

- A DNS server is deployed on the enterprise intranet to store the mapping between server domain names and IP addresses. When Internet users access intranet servers using domain names, multiple access paths exist. In this case, the smart DNS technology is required to select the optimal path.
- As shown in the figure, when Internet user A accesses an intranet server using a domain name, user A sends a DNS request to the intranet DNS server. The DNS server returns the resolved address to user A. The firewall intelligently changes the resolved address in the DNS response packet to ensure that the address and user A address are on the same ISP network and prevent user A from accessing the Internet across ISPs. This inbound intelligent uplink selection mode is called smart DNS.
- Smart DNS can be implemented in ISP egress mode, round robin mode, or weighted round robin mode. Based on the number of servers, there are two scenarios: single-server smart DNS and multi-server smart DNS.



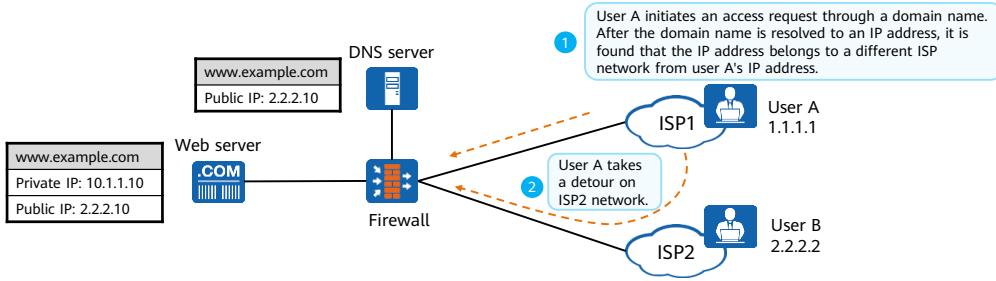
24 Huawei Confidential

 HUAWEI

- ISP egress mode: The firewall uses the smart DNS mapping table to change the IP address in the DNS response packet to the same ISP public address as the user, preventing traffic diversion.
- Round robin or weighted round robin mode: The firewall uses the round robin or weighted round robin algorithm to allocate different addresses to users based on weights. The firewall changes the destination addresses of user access requests to divert traffic to web servers over various links, implementing load balancing.

Single-Server Smart DNS Scenario

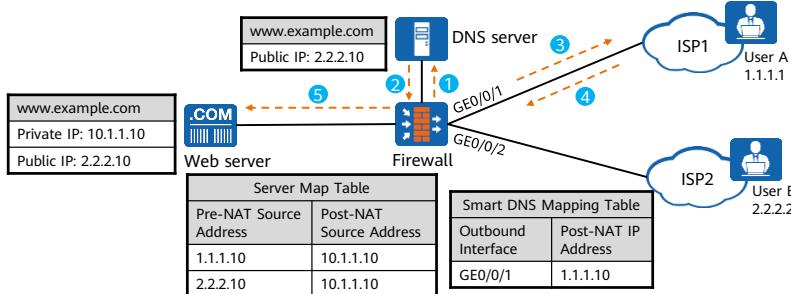
- Single-server smart DNS: When only one web server is deployed on the enterprise intranet, that is, the domain name of the web server on the DNS server of the enterprise intranet corresponds to the IP address of one web server, you need to configure single-server smart DNS.
- The following figure shows the user access path in the single-server scenario. Problems such as suboptimal path and link congestion exist. To solve them, configure ISP egress-based single-server smart DNS for ISP1 users.



- As shown in the figure, the enterprise or data center is connected to multiple ISP networks through several links. The private address of the web server is 10.1.1.10, and the public address of the web server is 2.2.2.10. The intranet DNS server has only mappings between the domain names (such as `www.example.com`) and public addresses (such as 2.2.2.10). When users on ISP1 access a web server on the intranet through domain name `www.example.com`, the domain name is mapped to IP address 2.2.2.10. The firewall then uses the NAT Server function to translate the destination address of packets from 2.2.2.10 to the private address (10.1.1.10) of the web server.
- When smart DNS is not configured and a user from another ISP network (such as an ISP1 user) accesses the web service provided by the enterprise through domain name `www.example.com`, the address that the DNS server provides after domain name resolution is 2.2.2.10, which resides on a different ISP network as the user's IP address (the ISP1 user address is 1.1.1.1). Therefore, the traffic of the ISP1 user needs to take a detour on ISP2 network to reach the web server, which increases the service access latency and inter-ISP settlement. Besides, all traffic from Internet users to the web server is forwarded over ISP2 network. This may cause network congestion on the link from the firewall to ISP2 network, but other links (such as ISP1 link) are idle.

Single-Server Smart DNS - ISP Egress Mode

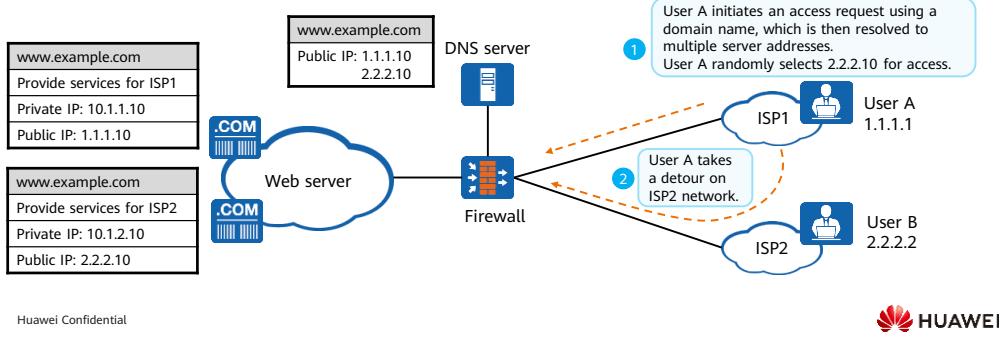
- After ISP egress-based single-server smart DNS is configured, the firewall changes the server address returned to an ISP1 user to an ISP1 network address (for example, 1.1.1.10 obtained from ISP1 network). In this way, the ISP1 user can access the web server directly from ISP1 network without taking a detour on the ISP2 network.
- As shown in the figure, it is assumed that the ISP egress-based smart DNS function is configured for ISP1 users on the firewall. The firewall maps the resolved address in the DNS response packet with the outbound interface of GE 0/0/1 to 1.1.1.10. The process for an ISP1 user to access the web server is as follows:



- The procedure is as follows:
 - The ISP1 user sends a DNS request to access the web server through domain name www.example.com.
 - The DNS server returns resolved IP address 2.2.2.10.
 - According to the smart DNS mapping table, the firewall changes the IP address in the DNS response packet to 1.1.1.10 that belongs to the same ISP network as the ISP1 user. Outbound interface GE 0/0/1 in the mapping table is mapped to address 1.1.1.10.
 - The ISP1 user initiates a packet destined to 1.1.1.10 for access. The packet reaches the firewall through ISP1 network.
 - With the NAT Server function, the firewall translates the destination address (1.1.1.10) of the packet into the private address (10.1.1.10) of the web server.
- As for users on ISP2 network, the firewall retains the address returned by the DNS server unchanged, still 2.2.2.10. With the NAT Server function, the firewall translates the destination address (2.2.2.10) of the packet into the private address (10.1.1.10) of the web server. Then ISP2 users can access the web server through ISP2 network. In this way, the situation in which the ISP1 link is idle while the ISP2 link is congested no longer exists, increasing the user access speed and enhancing user experience.

Problems in the Scenario with Multiple DNS Servers

- Multi-server smart DNS: When multiple web servers are deployed on the enterprise intranet, that is, the domain name of the web server on the DNS server of the enterprise intranet corresponds to the IP addresses of multiple web servers, you need to configure multi-server smart DNS.
- The following figure shows the user access path in the multi-server scenario. Problems such as suboptimal paths and extra settlement costs exist. To solve them, configure ISP egress-based multi-server smart DNS for ISP1 users.

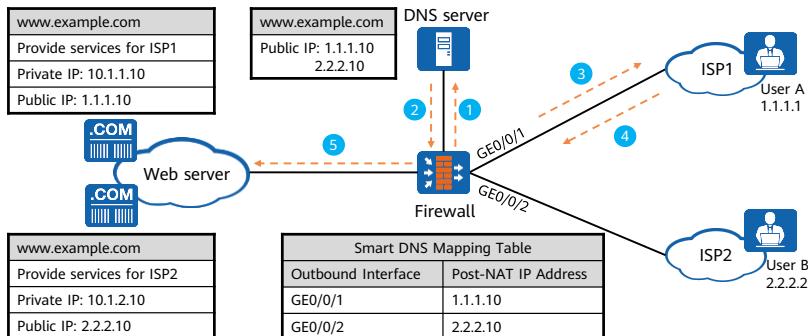


27 Huawei Confidential

- As shown in the figure, a large enterprise or data center provides the web service (such as website access) for external users and usually provides multiple web server addresses (1.1.1.10 and 2.2.2.10) for users on different ISP networks to access. The DNS server of the enterprise or data center has the mapping between the web service domain name and multiple server addresses.
- If smart DNS is not configured and a user of one ISP (such as ISP1) enters a domain name (such as `www.example.com`) to access the web service, the user initiates a DNS request to the DNS server on the intranet. The DNS server resolves the domain name and returns multiple server addresses (1.1.1.10 and 2.2.2.10) to the user. The ISP1 user selects one of them randomly to initiate the access, but the selected server address may belong to the other ISP (the ISP1 user may accidentally select the ISP2 server address 2.2.2.10). As a result, the ISP1 user needs to take a detour on ISP2 network before reaching the server, which increases the service access latency and inter-ISP settlement.

Multi-Server Smart DNS - ISP Egress Mode

- If you configure the ISP egress-based smart DNS, the firewall will return only one server address to each user, and the server address is on the same ISP network as the user address. In this way, the user does not need to take a detour on other ISP networks to access the web server.



28 Huawei Confidential

HUAWEI

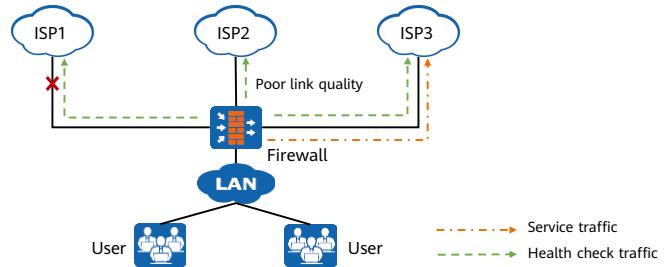
- The procedure is as follows:
 1. The ISP1 user sends a DNS request to access the web server through domain name www.example.com.
 2. The DNS server returns resolved IP addresses 1.1.1.10 and 2.2.2.10.
 3. According to the smart DNS mapping table, the firewall changes the IP address in the DNS response packet to 1.1.1.10. Outbound interface GE0/0/1 in the mapping table is mapped to address 1.1.1.10.
 4. The ISP1 user sends a packet destined for IP address 1.1.1.10 for access. The packet then reaches the firewall. In this way, the ISP1 user can access the web server directly from ISP1 network without taking a detour on ISP2 network, which increases the user access speed and user experience.
 5. With the NAT Server function, the firewall translates the destination address (1.1.1.10) of the packet into the private address (10.1.1.10) of the web server.
- As shown in the figure, ISP egress-based smart DNS is configured for ISP1 users on the firewall. The firewall maps the resolved address in the DNS response packet with outbound interface GE0/0/1 to 1.1.1.10, and maps the resolved address in the DNS response packet with outbound interface GE0/0/2 to 2.2.2.10. The following uses an ISP1 user's access to the web server as an example to describe the process of accessing the web server.
- Similarly, when an ISP2 user accesses the web server through domain name www.example.com, the firewall changes the IP address in the DNS response packet to 2.2.2.10 according to the smart DNS mapping table. The ISP2 user then sends a packet destined to IP address 2.2.2.10 for access. With the NAT Server function, the firewall translates the destination IP address (2.2.2.10) of the packet into the private address (10.1.2.10) of the web server.

Contents

1. Overview of Intelligent Uplink Selection
2. **Principles of Intelligent Uplink Selection**
 - Outbound Intelligent Uplink Selection
 - Inbound Intelligent Uplink Selection
 - Health Check
3. Configuration of Intelligent Uplink Selection

Overview of Health Check

- Health check is to probe the service or link availability or the link latency and adjust traffic distribution based on probe results to guarantee service quality.
- The firewall detects network changes in real time based on the health check result and takes measures immediately to ensure server or link availability. When multiple servers or links are available, the firewall can select the server with the optimal performance to process service traffic based on the service type or select the link that best meets the requirements based on the link latency, jitter, and packet loss ratio, improving user experience.



Protocols and Principles of Health Check

- The firewall sends probe packets to the specified devices on each ISP network. If a link connected to an outbound interface is available, the firewall can receive a response packet from the probed device; otherwise, the firewall cannot receive response packets. To prevent misjudgment caused by the fault of a probed device, the firewall can send probe packets to multiple devices through one outbound interface. The firewall determines that a link is available only if the number of response packets received through the link reaches the specified value.
- The firewall sends probe packets to destination devices using different protocols based on the device types and analyzes the response packets to evaluate the availability of the links.

Protocol	Principle
DNS	DNS is used to send a request packet to a specific device. If the Transaction ID in the request packet is the same as that in the response packet, the link is available.
HTTP	After the TCP three-way handshake, the firewall uses HTTP to send a request to the specified device to obtain the specified destination root directory. If the firewall receives an HTTP response packet, the link is available. Then the firewall sends an RST packet to terminate the TCP connection.
ICMP	The firewall sends an ICMP request to a specific device through a link. If the ICMP response packet returned by the device contains the same Identifier and Sequence number fields as the request packet, the firewall considers the link available.
RADIUS	RADIUS is used to send an authentication request to a specific server. In the request, the user name is guest , and password is empty. If the Identifier field in the request is the same as that in the response, the service is available.
TCP	The firewall sends a TCP connection request to the specified device. If the connection is established, the link is available. Then the firewall sends an RST packet to terminate the TCP connection.
TCP (simple probe)	TCP packets are used to check the network connectivity. A link is considered available upon the response to the first probe packet by the destination device, without requiring the three-way handshake.

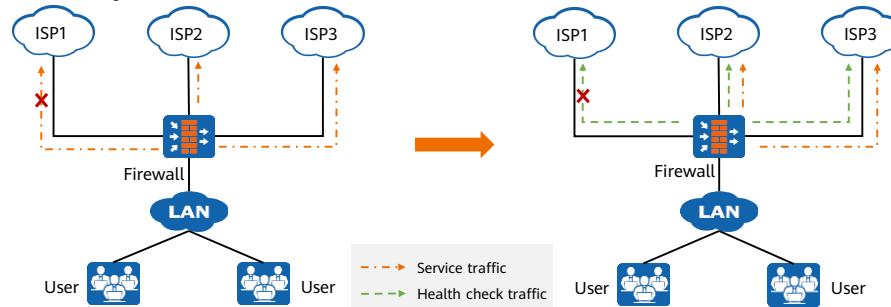
Link Quality Parameters

- Link quality parameters include the packet loss ratio, latency, and jitter. The packet loss ratio is the most important parameter. If the packet loss ratio, latency, and jitter of two links are different, the firewall determines that the link with a smaller packet loss ratio has a higher quality.

Parameter	Calculation Method
Latency	The latency is calculated based on the formula: Latency = Time when a response packet is received - Time when a probe packet is sent. The average latency of the N probe packets sent by the firewall is the final latency.
Jitter	The absolute value of the difference between two consecutive probe latency is jitter. The average jitter of the N probe packets sent by the firewall is the final jitter.
Packet loss ratio	After sending multiple probe packets, the firewall counts the number of lost packets and calculates the packet loss ratio. The packet loss ratio is equal to the number of lost packets divided by the number of probe packets.

Application Scenarios of the Health Check

- To improve traffic forwarding reliability, intelligent uplink selection can function with health check to prevent traffic from being forwarded over a faulty link.
 - If the health check result shows that a link becomes faulty, the interfaces on the link will not be involved in intelligent uplink selection.
 - When the link recovers from the fault, the interfaces on the link will participate in intelligent uplink selection again and the link forwards the assigned traffic.



33 Huawei Confidential

 HUAWEI

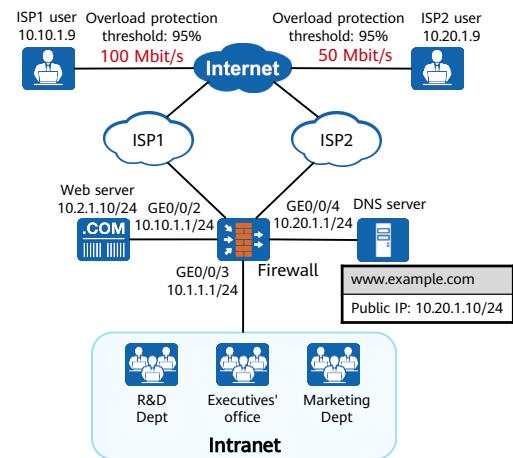
- As shown in the figure, in the global route selection scenario:
 - If health check is not enabled, the fault in ISP1 link cannot be detected. If ISP1 link is selected for traffic forwarding, user access will fail.
 - After health check is enabled, the firewall can detect any fault in ISP1 link. When intelligent uplink selection is triggered, ISP1 link will not participate in intelligent uplink selection. The firewall will select ISP2 or ISP3 link for traffic forwarding.

Contents

1. Overview of Intelligent Uplink Selection
2. Principles of Intelligent Uplink Selection
- 3. Configuration of Intelligent Uplink Selection**

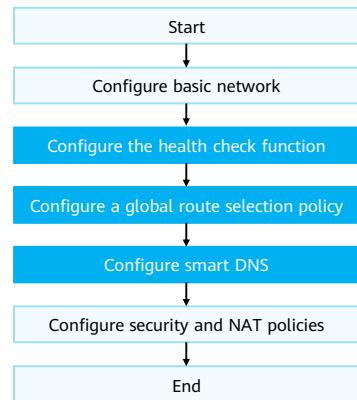
Examples for Configuring Intelligent Uplink Selection (1/2)

- Requirement description:
 - Assume that an enterprise has a 100 Mbit/s link connected to ISP1 and a 50 Mbit/s link connected to ISP2.
 - Traffic needs to be balanced between ISP1 and ISP2 links based on the bandwidth ratio to ensure that bandwidth resources are fully utilized.
 - When one ISP link is overloaded, subsequent traffic will be forwarded on the other ISP link to ensure access availability.
 - ISP1 users access the enterprise web server through ISP1 link, and ISP2 users access the enterprise web server through ISP2 link, preventing suboptimal paths.



Examples for Configuring Intelligent Uplink Selection (2/2)

- Configuration roadmap:
 - Complete basic network configurations, including configuring IP addresses for interfaces of the firewall, adding interfaces to security zones, and configuring default routes.
 - Configure the health check function to check the link status.
 - Configure a global route selection policy to implement load balancing by link bandwidth.
 - Configure smart DNS to allow Internet users to access the server through the optimal path.
 - Configure security and NAT policies to allow intranet users to access the Internet.



Configuring the Health Check Function

- Choose **Object > Health Check**. In the **Health Check List** area, click **Add** and create health checks for ISP1 and ISP2 as follows:

The figure consists of two side-by-side screenshots of a network configuration interface. Both screenshots show a 'Health Check List' configuration screen with a 'Detection Node List' table.

ISP1 Configuration (Left):

- Name: isp1_health (highlighted by red box 1)
- Check Interval: 5 seconds
- Maximum Attempts: 3
- Minimum Active Nodes: 1
- Source IP Address: (empty)
- Detection Node List:
 - Protocol: TCP (highlighted by red box 2)
 - Destination IP Address: 10.10.1.2
 - Port: 10001
 - Outgoing Interface: GE0/0/2

ISP2 Configuration (Right):

- Name: isp2_health (highlighted by red box 3)
- Check Interval: 5 seconds
- Maximum Attempts: 3
- Minimum Active Nodes: 1
- Source IP Address: (empty)
- Detection Node List:
 - Protocol: TCP (highlighted by red box 4)
 - Destination IP Address: 10.20.1.2
 - Port: 10002
 - Outgoing Interface: GE0/0/4

Configuring Interfaces

- Choose **Network > Interface**, set the link bandwidth and overload protection thresholds for the firewall interfaces connected to ISPs, and bind the corresponding health check.

GigabitEthernet0/0/2 Configuration:

- IP Address: 10.10.1.1/255.255.255.0
- Default Gateway: 10.1.1.254
- Health Check: isp1_health
- Interface Bandwidth:

Ingress Bandwidth: 100 Mbps	<1-1000>	Overload Protection Threshold: 95 %
Egress Bandwidth: 100 Mbps	<1-1000>	Overload Protection Threshold: 95 %

GigabitEthernet0/0/4 Configuration:

- IP Address: 10.20.1.1/24
- Default Gateway: 10.20.1.254
- Health Check: isp2_health
- Interface Bandwidth:

Ingress Bandwidth: 50 Mbps	<1-1000>	Overload Protection Threshold: 95 %
Egress Bandwidth: 50 Mbps	<1-1000>	Overload Protection Threshold: 95 %

Configuring Load Balancing by Link Bandwidth

- Choose **Network > Route > Intelligent Uplink Selection**. In the **Global Routing Policy** area, click **Edit**, and set load balancing by link bandwidth as follows:

The screenshot shows the 'Global Routing Policy' configuration page. At the top, under 'Selection Mode', 'Load balancing based on link bandwidth' is selected (marked with a red circle 1). Below this, 'Source Subnet Mask (bits)' is set to 32. In the 'Outgoing Interface List' section, two interfaces, GE0/0/4 and GE0/0/2, are listed with an overload protection threshold of 95 for both incoming and outgoing traffic (marked with a red circle 2).

WAN Interface/Carrier/Interface Group	Overload Protection Threshold		Edit
	Incoming	Outgoing	
GE0/0/4	95	95	<input checked="" type="checkbox"/>
GE0/0/2	95	95	<input checked="" type="checkbox"/>

Configuring Smart DNS on the Outbound Interface

- Choose **Network > DNS > Smart DNS**. Enable **Smart DNS** and click **Apply**.
 - In **Smart DNS List**, click **Add**. In the **Smart DNS List** area, click **Add**. On the **Add Smart DNS** page that is displayed, configure single-server smart DNS and change the **DNS Reply Address** from **10.20.1.10** to **10.10.1.10** (applied from ISP1).



Quiz

1. (Multiple-answer question) Which of the following load balancing modes are available in a global route selection policy? ()
 - A. Load balancing by link bandwidth
 - B. Load balancing by link quality
 - C. Load balancing by link weight
 - D. Active/standby backup by link priority

1. ABCD

Quiz

2. (Multiple-answer question) Which of the following types of PBR matching conditions are supported by the firewall? ()
 - A. Inbound interface
 - B. Service type
 - C. Application type
 - D. User

2. ABCD

Summary

- This course describes the intelligent uplink selection function of Huawei firewalls. Intelligent uplink selection allocates proper link access resources to enterprise users to implement link load balancing and improve network utilization.
- Upon completion of this course, you have had a basic understanding of the principles of intelligent uplink selection on the firewall and mastered the configurations related to intelligent uplink selection.

Recommendations

- Huawei official websites:
 - Enterprise service: <https://e.huawei.com/en/>
 - Technical support: <https://support.huawei.com/enterprise/en/index.html>
 - Online learning: <http://learning.huawei.com/en/>

Acronyms and Abbreviations

Acronym/Abbreviation	Full Name
ACL	Access Control List
DNS	Domain Name Service
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
ISP	Internet service provider
NAT	Network Address Translation
PBR	Policy-Based Routing
RADIUS	Remote Authentication Dial-In User Service
TCP	Transmission Control Protocol
SFTP	Secure File Transfer Protocol

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。
Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

Copyright©2022 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product performance, market position, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.



IPsec VPN Technology and Application



Foreword

- Most data is transmitted in cleartext on the Internet, causing security risks. For example, bank accounts and passwords may be intercepted or tampered with, user information may be forged, and bank networks may be attacked.
- After IPsec VPN is deployed in scenarios such as communication between enterprise branches and headquarters, data transmitted in such communication can be protected, reducing risks of information leakage.
- This course describes the basic principles, application scenarios, high reliability, and troubleshooting roadmap of IPsec.

Objectives

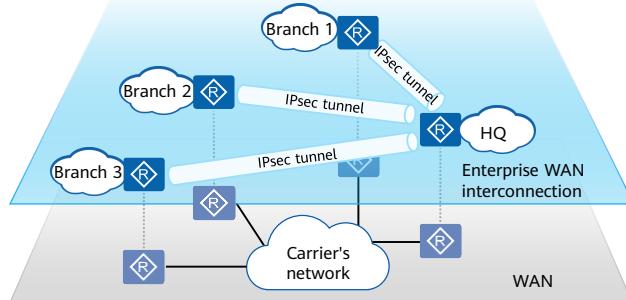
- On completion of this course, you will be able to:
 - Understand the basic principles of IPsec VPN.
 - Understand the typical application scenarios of IPsec VPN.
 - Master the highly reliable IPsec VPN configuration method.
 - Master IPsec VPN troubleshooting method.

Contents

- 1. Basic Principles of IPsec VPN**
2. Application Scenarios of IPsec VPN
3. High Reliability of IPsec VPN
4. Troubleshooting of IPsec VPN

Background of IPsec VPN

- Enterprise branches can use many interconnection modes to interconnect with each other, for example, WAN private lines or Internet.
- Some enterprises use the Internet for interconnection based on costs and requirements. However, security risks such as information leakage exist. Therefore, ensuring that data is not stolen or tampered during transmission becomes a major concern. IPsec tunnels can be established between branches and headquarters to encrypt data packets for secure interconnection.



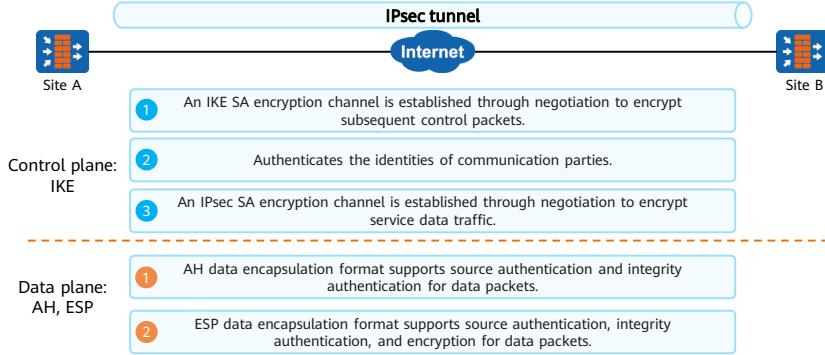
4 Huawei Confidential

 HUAWEI

- Leveraging encryption and authentication, IPsec secures service data transmission over the Internet through the following capabilities:
 - Data origin authentication: The receiver checks the validity of the sender.
 - Data encryption: The sender encrypts data packets and transmits them in cipher text on an open network. The receiver decrypts or directly forwards the received data packets.
 - Data integrity: The receiver verifies the received data to determine whether the packets have been tampered with during transmission.
 - Anti-replay: The receiver rejects old or duplicate data packets to prevent malicious users from launching attacks by repeatedly sending obtained packets.

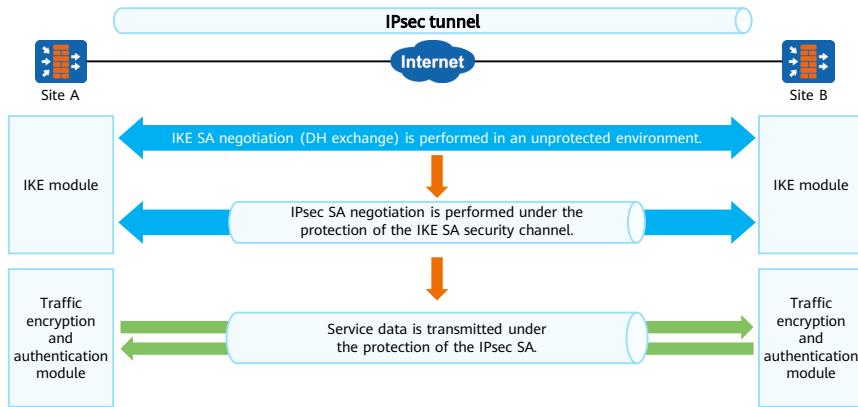
IPsec Framework

- IPsec is a set of open network security protocols defined by the Internet Engineering Task Force (IETF). It is not a single protocol, but a collection of protocols and services that provide security for IP networks.
- The IPsec protocol framework consists of three standard protocols: IKE, AH, and ESP whose functions are as follows:



IKE SA and IPsec SA

- IPsec peers need to negotiate two types of SAs: IKE SA and IPsec SA. The negotiation sequence is as follows:



6 Huawei Confidential

 HUAWEI

- In a typical IPsec communication model, one IKE SA and two IPsec SAs need to be established.
- The figure above shows the relationship between IKE SA and IPsec SA. Two peers establish an IKE SA for identity authentication and key exchange. Protected by the IKE SA, the peers negotiate a pair of IPsec SAs using the configured AH or ESP protocol and other parameters. Subsequently, service data is encrypted and transmitted between the peers in an IPsec SA tunnel.

Key Parameters of IKE SA

- IKE has two versions: IKEv1 and IKEv2. The table below lists the parameters negotiated by IPsec peers for establishing an IKE SA tunnel.
- Only one IKE SA needs to be established between IPsec peers to implement two-way data transmission.

Parameter	IKEv1	IKEv2	Description
IKE working mode	Main mode or aggressive mode	/	IKEv1 has two working modes.
DH group	14, 15, 16, 18, 19, 20, 21, 22, etc.		DH algorithm is used to negotiate symmetric keys.
Encryption algorithm	DES, 3DES, AES	DES, 3DES, AES	Used for IKE SA packet encryption.
Authentication algorithm	MD5, SHA1, SHA2	MD5, SHA1, SHA2	Used for IKE SA packet authentication.
Authentication mode	Pre-shared key, RSA signature, RSA digital envelope		Used for identity authentication of IPsec peers.
Timeout interval	The default value is 86400 seconds.		IKE SA lifetime.
PRF algorithm	/	MD5, SHA1, SHA2, etc.	IKEv2 PRF algorithm.

- IKEv2 establishes an IKE SA through the initial exchange and does not involve the working mode.
- DH is a public key exchange method that generates keying materials and uses ISAKMP messages to exchange keying materials between the sender and receiver. Then, the devices at both ends calculate the same symmetric key. The symmetric key is used for encryption and authentication.
- Encryption algorithm: The DES and 3DES encryption algorithms are insecure. You are advised to use the AES algorithm.
- Authentication algorithm: The MD5 and SHA1 authentication algorithms are insecure. You are advised to use the SHA2-256, SHA2-384, SHA2-512 algorithms.
- The PRF algorithm (default HMAC-SHA2-256) is used in IKEv2 negotiation.

Key Parameters of IPsec SA

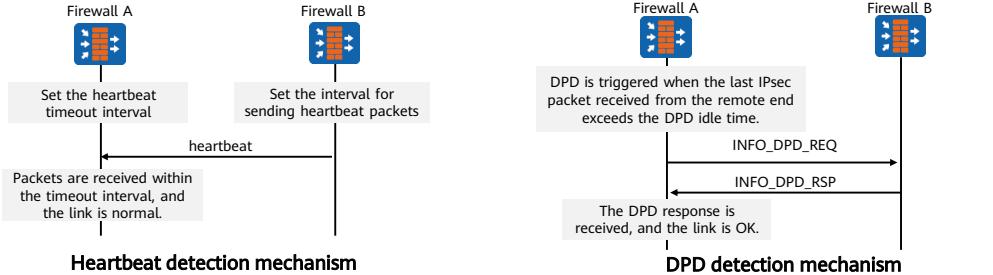
- An IPsec SA is used to encrypt service data. The negotiation process is protected by the IKE SA encryption security channel. The following table lists the negotiation parameters.
- At least two IPsec SAs must be established between IPsec peers to implement two-way encrypted data transmission (IPsec SAs are one-way).

Parameter	AH	ESP	Description
Traffic to be protected	Only authentication is supported while encryption is not supported.	Authentication and encryption are supported.	Negotiate which data flows need to be protected.
Encapsulation mode	Transport mode and tunnel mode		Transport mode: No new IP header is added. Tunnel mode: A new IP header is added.
Encryption algorithm	/	DES, 3DES, AES, GMAC, GCM, etc.	Used for IPsec SA packet encryption.
Authentication algorithm		MD5, SHA1, SHA2, etc.	Used for IPsec SA packet authentication.
PFS	Whether to perform additional DH exchange to negotiate the symmetric key of the IPsec SA.		PFS enhances the security of IPsec SAs.
Timeout interval	Time-based: 3600 seconds by default Traffic-based: 5242880 KB by default.		IPsec SA lifetime.

- Perfect Forward Secrecy (PFS) indicates that the symmetric key used for the IPsec SA is generated through single separate DH exchange and does not depend on the IKE SA. In this way, even if the key of the IKE SA is cracked, the security of the IPsec SA is not affected.

IKE SA Status Detection Mechanism

- IKE does not provide a peer status monitoring mechanism. When one peer is unreachable, the other cannot detect the fault. As a result, data traffic forwarded to the remote end is discarded. To quickly detect the IKE peer status, the device provides two IKE peer status detection mechanisms: heartbeat and DPD.
 - Heartbeat detection: The local end periodically sends heartbeat packets to the remote end.
 - DPD detection: If the local end does not receive IPsec traffic from the remote end within a specified period, the local end sends DPD packets to detect the status of the remote end.



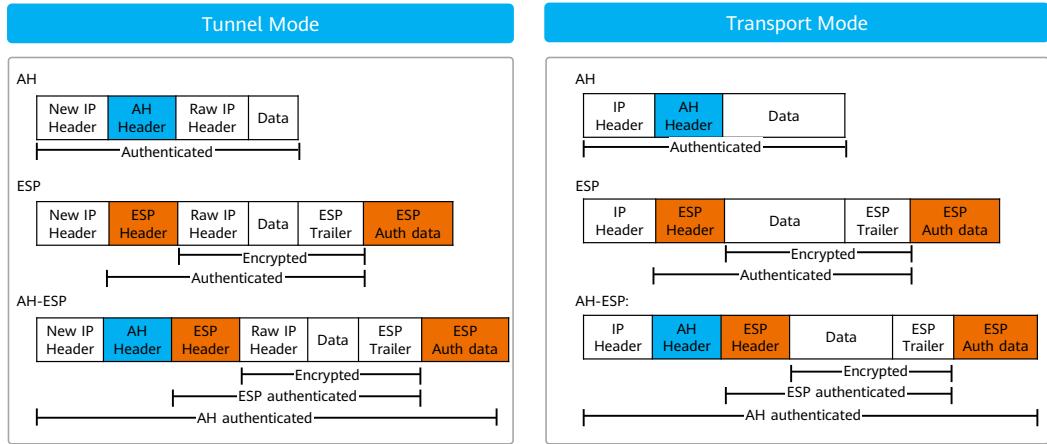
9 Huawei Confidential

 HUAWEI

- DPD has the following detection modes:

- On-demand DPD: If the local end needs to send IPsec packets to the remote end, it sends a DPD request packet to the remote end when it determines that the time since it received the last IPsec packet from the remote end exceeds the DPD idle time.
 - Periodic DPD: If the time since the local end received the last IPsec packet or DPD request packet from the remote end exceeds the DPD idle time, the local end sends a DPD request packet to the remote end.

IPsec Data Encapsulation Mode



10 Huawei Confidential



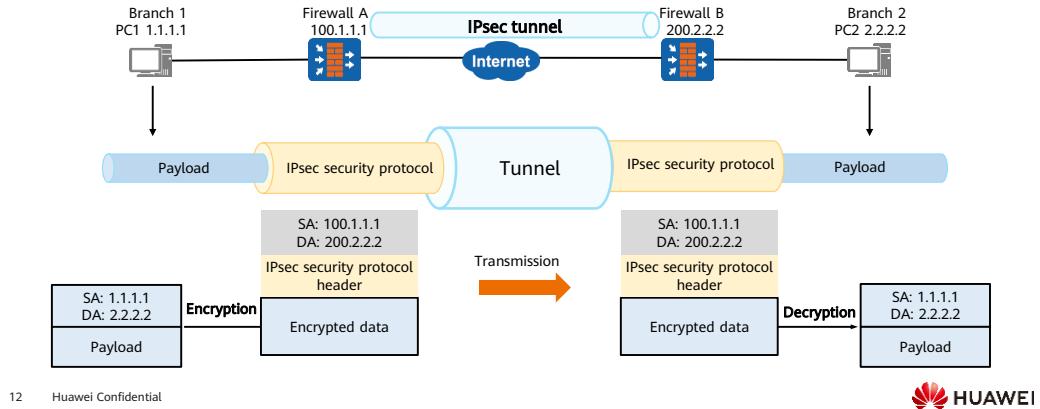
- In transport mode, an AH or ESP header is added between an IP header and a transport-layer protocol (TCP, UDP, or ICMP) header to protect the TCP, UDP, or ICMP payload. As no additional IP header is added, IP addresses in the original packets are visible in the IP header of the post-encrypted packet.
- In tunnel mode, an AH or ESP header is added before the raw IP header and then encapsulated into a new IP packet with a new IP header to protect the IP header and payload.
- In tunnel mode, AH checks the integrity of the entire IP packet including the new IP header. ESP checks the integrity of the ESP header, original IP header, transport-layer protocol header, data, and ESP trailer, excluding the new IP header. As such, ESP cannot protect the new IP header. ESP encrypts the original IP header, transport-layer protocol header, data, and ESP trailer.

Comparison Between AH and ESP

Security Protocol	AH	ESP
Protocol ID	51	50
Data integrity check	Supported (checking the entire IP packet)	Supported (not checking the IP header)
Data origin authentication	Supported	Supported
Data encryption	Not supported	Supported
Anti-replay	Supported	Supported
NAT traversal	Not supported	Supported

IPsec VPN

- IPsec data can be encapsulated in transport mode or tunnel mode. In tunnel mode, VPN functions can be implemented in addition to protecting data traffic. This mode is called IPsec VPN. The following figure shows a typical application scenario where IPsec VPN is used for encrypted communication between branch 1 and branch 2.



Contents

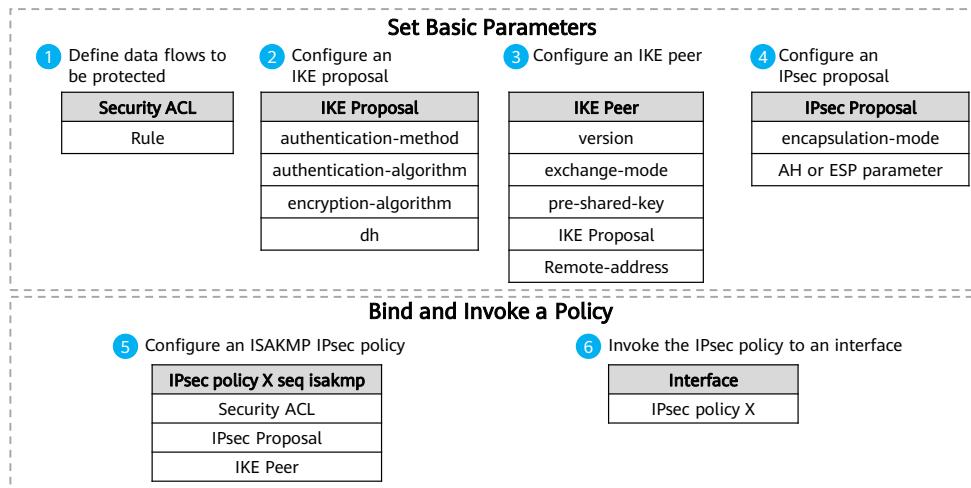
1. Basic Principles of IPsec VPN
2. Application Scenarios of IPsec VPN
 - Site-to-Site Application Scenario
 - Site-to-Multisite Application Scenario
 - GRE over IPsec Application Scenario
 - Certificate Authentication Scenario
 - NAT Traversal Scenario
3. High Reliability of IPsec VPN
4. Troubleshooting of IPsec VPN

Site-to-Site Application Scenario of IPsec VPN

- A site-to-site IPsec VPN, also called a LAN-to-LAN IPsec VPN or gateway-to-gateway IPsec VPN, is used to establish an IPsec tunnel between two gateways, implementing secure communication between LANs.
- This network requires that two gateways on both ends of the tunnel have fixed IP addresses or fixed domain names, and either end can initiate a connection.



Configuration Roadmap



- This section uses the IPsec IKEv1 configuration process as an example. The IKE peer in IKEv2 does not have the **exchange-mode**. For details about the security policy configuration, see the configuration manual.

Key Configuration (1/2)

- Choose **Network > IPSec > IPSec** and click **Add** to create an IPsec policy in ISAKMP mode (site-to-site scenario).

The screenshot shows the 'Add IPsec Policy' configuration page. The 'Scenario' section is set to 'Site-to-site'. The 'Basic Configuration' section includes a 'Policy Name' (policy1), 'Local Interface' (GE0/0/1), and 'Local Address' (1.1.1.1). The 'Peer Address' field is empty. The 'Authentication Type' section uses 'Pre-shared key' with a password of '*****'. The 'Data Flow to Encrypt' table lists a rule: Source '192.168.10.0/24' to Destination '192.168.20.0/24' with 'any' ports and 'any' action, marked as 'Encrypt'. The 'IKEIPSec Proposal' section is collapsed.

Key Configuration (2/2)

- Configure an IPsec policy and select IKE and IPsec parameters.

IKE/IP Sec Proposal

Advanced

IKE Parameters

IKE Version: V1 V2 (V2 is used to initiate negotiations. Either IKEv1 or IKEv2 is used to accept negotiations.)

Negotiation Mode: Automatic Main Aggressive

Encryption: SM4 AES-256 AES-192 AES-128

Authentication: SM3 SHA2-512 SHA2-384 SHA2-256

Integrity Hash: SHA2-512 SHA2-384 SHA2-256 AES-128

PRF: 24 21 20 19

DH Group: 18 16 15 14

SA Timeout: 86400 <60-604800>seconds

IPSec Parameters

Encapsulation Mode: Automatic Transport Tunnel

Security Protocol: ESP AH AH-ESP

ESP Encryption: SM4 GCM256 GCM192 GCM128

GMAC256 GMAC192 GMAC128 AES-256

AES-192 AES-128

ESP Authentication: SM3 SHA2-512 SHA2-384 SHA2-256

PFS: NONE 24 21 20

19 18 16 15

SA Timeout: By Time (3600 <30-604800>Seconds) By Traffic (5242880 <0..256-200000000>KB)

Dead Peer Detection (DPD)

Detected Mode: Periodic On-demand

Detected Interval: 30 <10-3600>seconds

Retry Interval: 15 <2-60>seconds

Retrans Times: 3 <3-10>Times

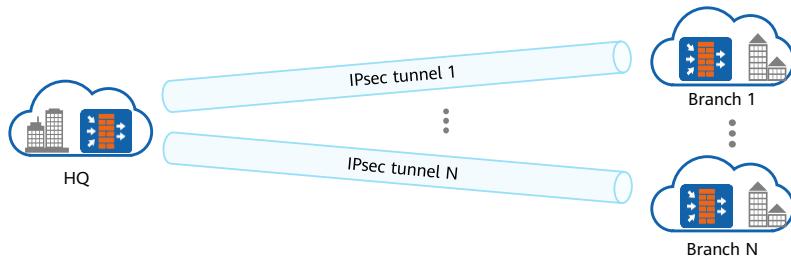
Buttons: Apply Return

Contents

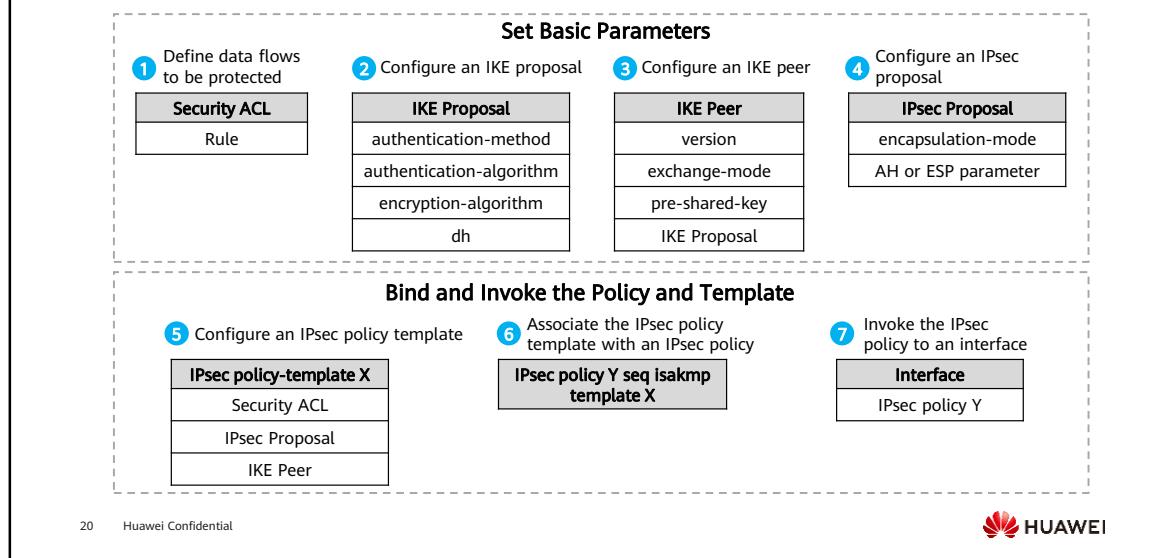
1. Basic Principles of IPsec VPN
2. **Application Scenarios of IPsec VPN**
 - Site-to-Site Application Scenario
 - **Site-to-Multisite Application Scenario**
 - GRE over IPsec Application Scenario
 - Certificate Authentication Scenario
 - NAT Traversal Scenario
3. High Reliability of IPsec VPN
4. Troubleshooting of IPsec VPN

Site-to-Multisite Application Scenario of IPsec VPN

- Site-to-multisite VPN is suitable when an HQ needs to set IPsec VPN tunnels with multiple branches. When the HQ and branches are connected in hub-spoke architecture, the branches establish IPsec tunnels with the HQ, and the communications between the branches is forwarded and controlled by the HQ.



Configuration Roadmap - Template



- When the traditional site-to-site IPsec VPN configuration mode is used, the remote IP address must be specified. In many scenarios, one end (such as small branches and stores) of the IPsec VPN does not have a public IP address or a fixed IP address. If there are a large number of branches, the headquarter needs to maintain a configuration for each branch. The configuration workload of the headquarter will be heavy. In this case, you can use an IPsec template to solve the preceding problems.
- IPsec template: The remote IP address is not limited. You can strictly specify the remote IP address (single IP address), specify the remote IP address (IP address segment), or do not specify the remote IP address (any IP address).
- This course describes only the IPsec configuration process. For details about security policy configurations, see the configuration manual.

Key Configuration

- Choose **Network > IPSec > IPSec** and click **Add** to create an IPsec policy in template mode (site-to-multipsite scenario).

Source	Destination	Proto...	Source Port	Destin...	Action
192.168.20.0/24	192.168.10.0/24	any	any	any	Encrypt

21 Huawei Confidential

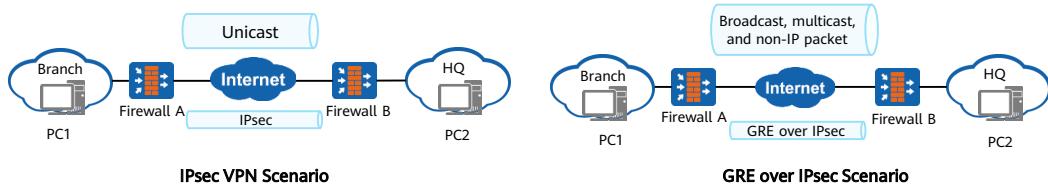


Contents

1. Basic Principles of IPsec VPN
2. **Application Scenarios of IPsec VPN**
 - Site-to-Site Application Scenario
 - Site-to-Multisite Application Scenario
 - **GRE over IPsec Application Scenario**
 - Certificate Authentication Scenario
 - NAT Traversal Scenario
3. High Reliability of IPsec VPN
4. Troubleshooting of IPsec VPN

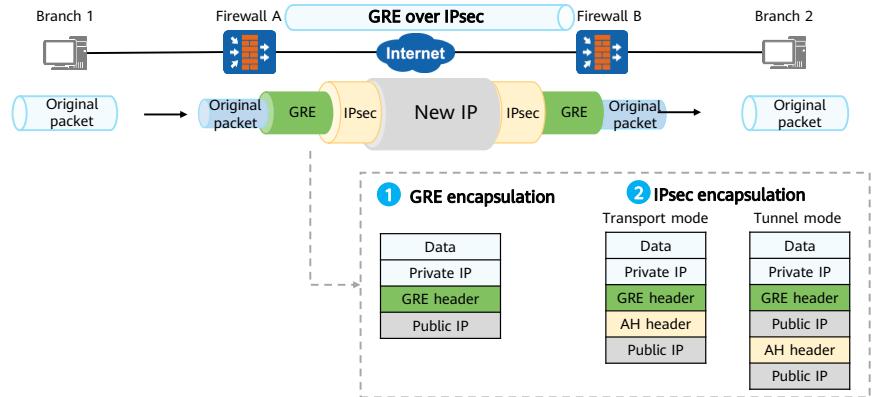
GRE over IPsec Application Scenario

- The local device of the IPsec VPN cannot detect the number of remote devices, and the local device shares an IPsec SA. The packet encapsulation does not contain the next hop of the remote device. Therefore, multicast, broadcast, and non-IP packets, such as OSPF packets, cannot be transmitted. As a result, OSPF routes cannot be used between the branch and headquarter networks.
- GRE over IPsec uses GRE to encapsulate multicast, broadcast, and non-IP packets into common IP packets, and uses IPsec to provide secure communication for encapsulated IP packets. In this way, broadcast and multicast services can be securely transmitted between the headquarters and branches.



GRE over IPsec Packet Encapsulation

- GRE over IPsec encapsulates packets using GRE and then IPsec. GRE over IPsec supports the transport and tunnel encapsulation modes. The process of encapsulating GRE over IPsec packets using AH is as follows:



24 Huawei Confidential

 HUAWEI

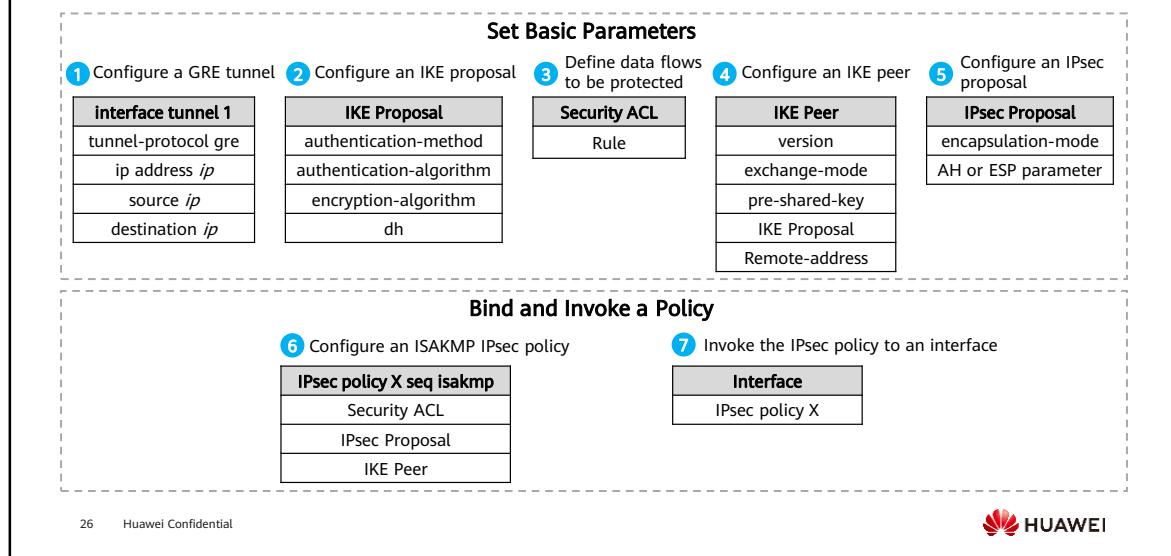
- GRE over IPsec packet encapsulation process:
 - GRE supports non-IP unicast packets, such as IPX packets and multicast packets. Original packets are encapsulated in GRE tunnels.
 - GRE tunnel encapsulated packets are encapsulated in IPsec tunnel encapsulated packets.

Advantages of GRE over IPsec

Feature	Supported by GRE	Supported by IPsec	Supported by GRE over IPsec
Multicast	Y	N	Y
Dynamic routing protocols	Y	N	Y
Various network layer protocols	Y	Limited support	Y
Confidentiality	N	Y	Y
Integrity	N	Y	Y
Data origin authentication	N	Y	Y

- Multicast: multicast packets;
- Dynamic routing protocols, such as OSPF and IS-IS. Some dynamic routing protocol packets are multicast or broadcast packets.
- Various network layer protocols: supports network layer protocols, such as IP, IPX, ARP, and ICMP.
- Confidentiality: packets can be encrypted.
- Integrity: received packets can be verified to check whether the packets are complete and modified.
- Data origin authentication: authenticates the source that receives data.

Configuration Roadmap of GRE over IPsec



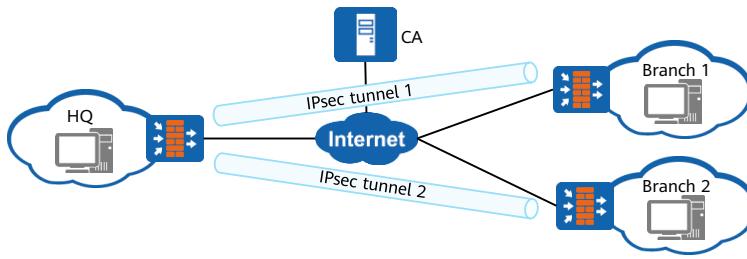
- The following uses IPsec VPN in ISAKMP mode as an example to describe how to configure site-to-site GRE over IPsec.

Contents

1. Basic Principles of IPsec VPN
2. **Application Scenarios of IPsec VPN**
 - Site-to-Site Application Scenario
 - Site-to-Multisite Application Scenario
 - GRE over IPsec Application Scenario
 - Certificate Authentication Scenario
 - NAT Traversal Scenario
3. High Reliability of IPsec VPN
4. Troubleshooting of IPsec VPN

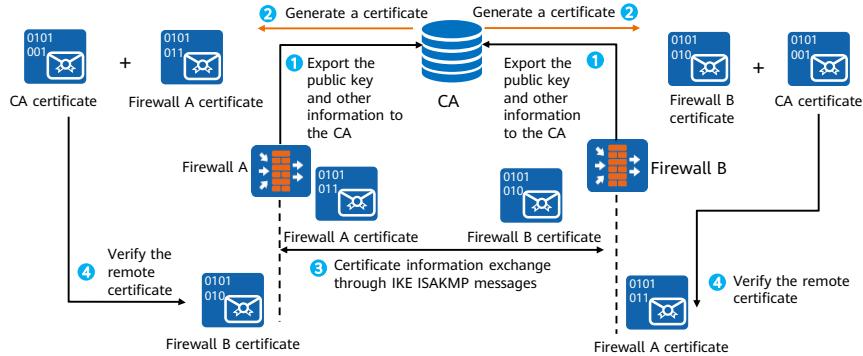
IPsec VPN Certificate Authentication Scenario

- In the IPsec VPN site-to-multisite scenario, if the pre-shared key mode is used for identity authentication, the pre-shared key must be configured for the peer between the headquarter and each branch. If all peers use the same key, security risks exist. If each peer uses a different key, it is difficult to manage and maintain the key.
- To solve the preceding problems, certificate authentication can be used. IKE uses the certificate mechanism of PKI to authenticate peers. Therefore, you do not need to configure an independent key for each peer, which reduces management costs.



Certificate Application on the IPsec VPN

- To use a certificate for identity authentication, perform the following steps:
 - Certificate import: Use the device key and necessary information to issue a certificate to the CA and import the certificate pair to the device.
 - Certificate authentication: During IPsec identity authentication, each sends the imported local certificate to the remote end for identity authentication.



Key Configuration - Applying for a Local Certificate on the Firewall

- Create a public/private key pair. Create a 2048-bit RSA key pair **rsa** and allow it to be exported.

```
[FW] pki rsa local-key-pair create rsakey exportable
```

- Configure a PKI entity.

```
[FW] pki entity user01
[FW-pki-entity-user01] common-name devicea
[FW-pki-entity-user01] country cn
[FW-pki-entity-user01] ip-address 10.1.61.11
[FW-pki-entity-user01] state Hangzhou
[FW-pki-entity-user01] organization huawei
[FW-pki-entity-user01] organization-unit Training
[FW-pki-entity-user01] quit
```

- Configure offline local certificate application for the PKI entity. During local certificate application, the IP address in the application file must be set to the IP address used by the firewall when the IPsec tunnel is established.

```
[FW] pki realm abc
[FW-pki-realm-abc] entity user01
[FW-pki-realm-abc] rsa local-key-pair rsakey
[FW-pki-realm-abc] quit
[FW] pki enroll-certificate realm abc pkcs10 filename cer_req
```

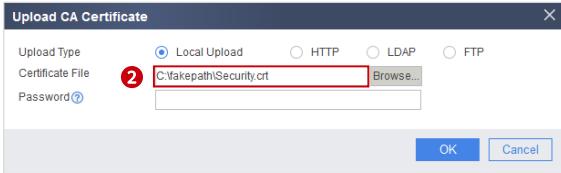
- Configure an RSA key pair. Before applying for a local certificate, you need to configure the RSA key pair to generate a public key and a private key. The public key is sent by the PKI entity to CA, and the remote end uses this key to encrypt cleartext. The private key is kept by the PKI entity itself and used to digitally sign and decrypt the ciphertext from the remote end.
- After the configurations are complete, run the display pki cert-req command to view content of the certificate request file.
- When the local certificate is successfully registered, download the local certificate in out-of-band mode. Transfer the certificate file to the device storage using a file transfer protocol.

Key Configuration - Importing Local and CA Certificates

- After the certificate application is complete, choose **Object > Certificate > Local Certificate** to import the certificate.

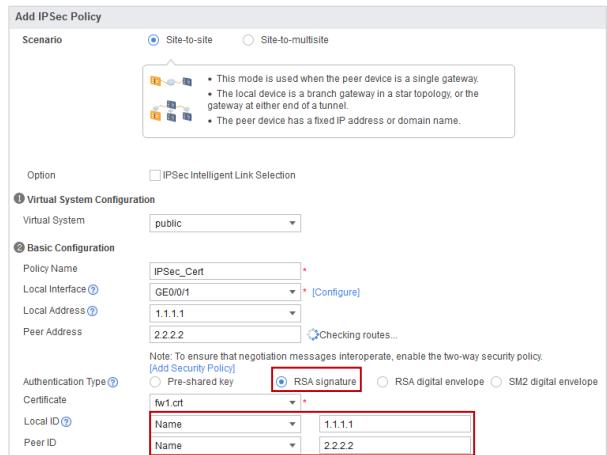


- Choose **Object > Certificate > CA Certificate** to import the certificate.



Key Configuration - RSA Signature Authentication

- Choose **Network > IPsec > IPsec**. In IPsec policy list, click **Add**.
- Set the parameters in the **Basic Configuration** area as follows:
 - Set **Authentication Type** to **RSA Signature**.
 - Select the imported certificate for verification. The local ID and remote ID must be the same as those entered during certificate application.



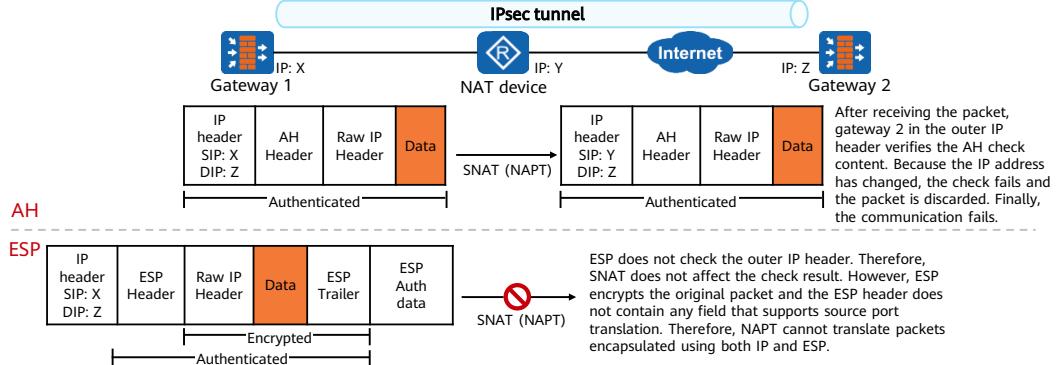
- If you select RSA digital envelope, you need to import both the local certificate and the remote certificate. Some information in the certificate will be sent to the remote end during tunnel establishment. In this way, both ends can verify the validity of the remote end.

Contents

1. Basic Principles of IPsec VPN
2. **Application Scenarios of IPsec VPN**
 - Site-to-Site Application Scenario
 - Site-to-Multisite Application Scenario
 - GRE over IPsec Application Scenario
 - Certificate Authentication Scenario
 - NAT Traversal Scenario
3. High Reliability of IPsec VPN
4. Troubleshooting of IPsec VPN

Problems of IPsec VPN in NAT Scenarios

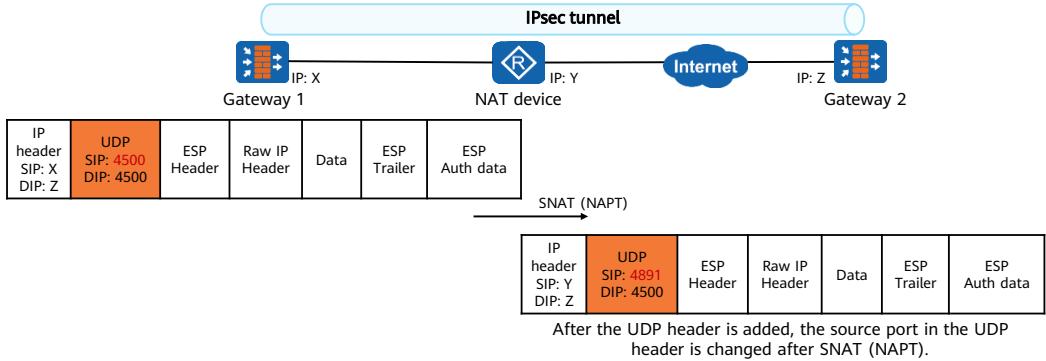
- By default, the ESP header or AH header is above the outer IP header during IPsec VPN data transmission. Problems may occur in transport mode and tunnel mode when a source NAT device exists on the transmission path.
- The following figure uses the tunnel mode as an example.



- The AH protocol does not support NAT traversal. The ESP protocol is restricted by ports and requires additional ports.

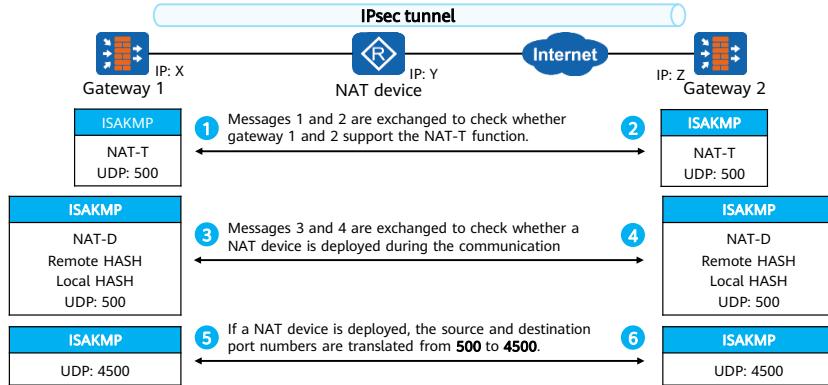
Overview of NAT Traversal

- To solve the preceding problem, you must enable the NAT traversal function on the two gateways that establish the IPsec tunnel.
- After NAT traversal is enabled, if a NAT device is detected between two gateways (detected during IKE process), ESP packets are encapsulated in a UDP header with the source and destination port numbers being 4500 to support NAT.



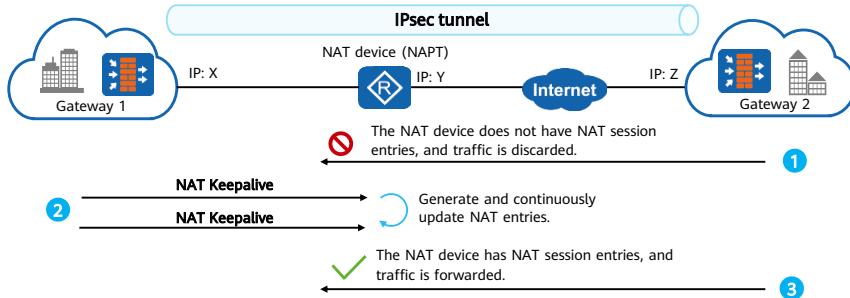
Detection Mechanism of NAT Traversal

- The IKEv1 main mode is used as an example to describe the NAT traversal detection mechanism.



Session Keepalive Mechanism for NAT Traversal

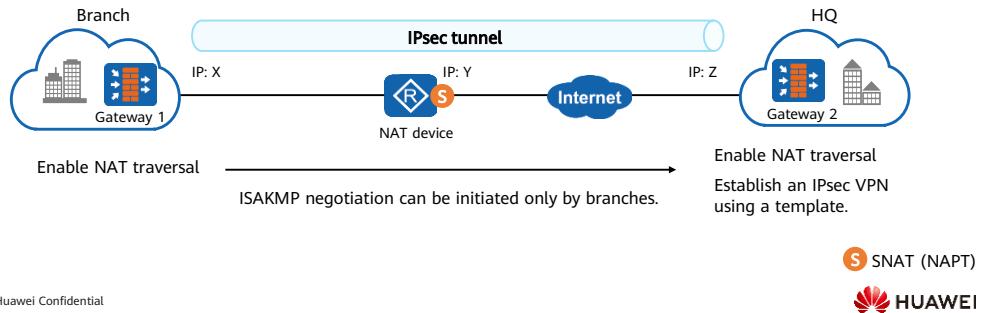
- The following figure shows the NAPT scenario. Gateway 1 is located behind the NAT device. If gateway 1 does not initiate an access request, the NAT device does not have a NAT session entry. In this case, gateway 2 cannot access gateway 1.
- To solve the preceding problems, enable the NAT session keepalive function on gateway 1. After this function is enabled, gateway 1 periodically sends NAT keepalive packets so that the NAT device generates and maintains NAT entries. In this way, gateway 2 can proactively access gateway 1.



- The format of the NAT keepalive packet is simple. The UDP header is followed by two hexadecimal Fs, which are used to update NAT session entries.
- After the Huawei firewall detects that the IPsec VPN is in the NAT traversal scenario, the internal device (initiator gateway 1) of the NAT device periodically sends NAT keepalive packets to ensure that the source NAT session on the intermediate NAT device does not age.

NAT Traversal Scenario (1/3)

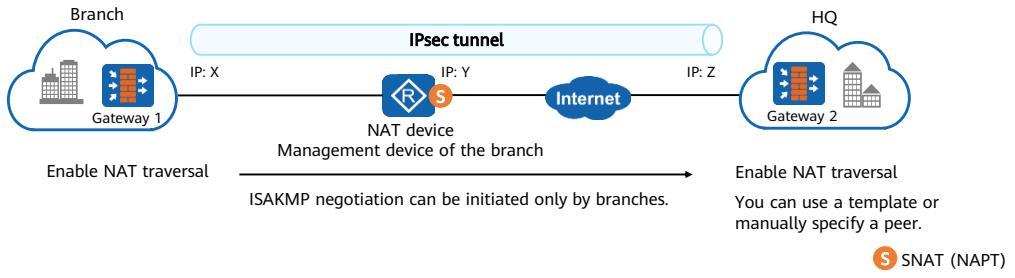
- In this scenario, the NAT device is located outside the branch network. The private IP address X of the outbound interface of branch gateway 1 is translated into the public IP address Y by the NAT device. The headquarter cannot obtain the public IP address of the branch after NAT. Therefore, the remote public IP address cannot be specified on the gateway 2. Therefore, IPsec must be configured on the gateway 2 using a template, and NAT traversal must be enabled on the gateways of both the headquarter and branch.
- Since the headquarter uses a template IPsec policy, it cannot initiate access to the branch and only the branch can initiate ISAKMP negotiation with the headquarter.



- In this scenario, the branch gateway is a firewall, and the public IP address of the NAT device is invisible to the headquarter. Therefore, you need to use a template to establish an IPsec tunnel. Although a NAT device is deployed between the branch and headquarter, the security policy configuration of the firewall is the same as that in the non-NAT traversal scenario.
- According to the security zone division rules of gateway 1 and gateway 2, the zone connected to the internal network is the Trust zone; the zone connected to the external network is the Untrust zone, and the IP address of the device is the Local zone. The security policy configuration is as follows:
 - Security policy of gateway 1:
 - Local -> Untrust, IP address of gateway 1: X -> IP address of gateway 2: Z;
 - Trust -> Untrust, branch intranet address -> HQ intranet address;
 - Untrust -> Local, IP address of gateway 2: Z -> IP address of gateway 1: X.
 - Security policy of gateway 2:
 - Local -> Untrust, IP address of gateway 2: Z -> any;
 - Trust -> Untrust: intranet IP address of the HQ -> intranet IP address of the branch;
 - Untrust -> Local, any -> IP address of gateway 2: Z.

NAT Traversal Scenario (2/3)

- In this scenario, the NAT device is located outside the branch network. The private IP address X of the outbound interface of branch gateway 1 is translated into the public IP address Y by the NAT device. The NAT device is the management device of the branch, and the public IP address is fixed. In this case, the translated public IP address is known. Therefore, the headquarter can use a template or manually specify a peer to configure IPsec VPN.
- The NAT device only translates the source address. Therefore, only the branch can initiate ISAKMP negotiation.

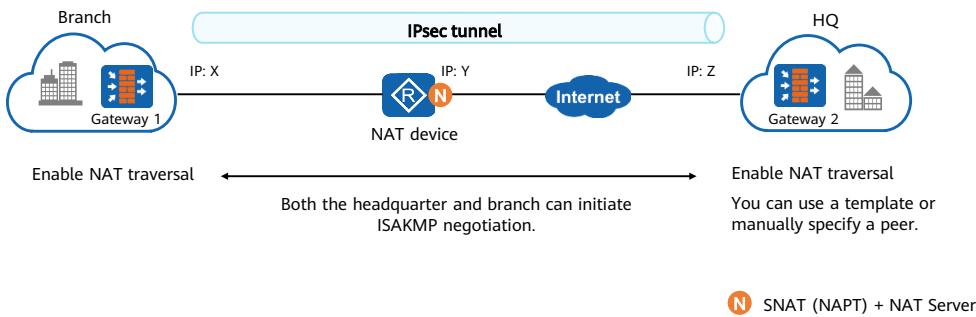


39 Huawei Confidential

- In this scenario, the branch gateway is a firewall, the public IP address of the NAT device is fixed, and the headquarter knows the public IP address of the NAT device. Therefore, you can configure IPsec using a template or manually specify a peer. In this case, a NAT device is deployed between the branch and headquarter; therefore, the firewall security policy configuration is different from that in non-NAT traversal scenarios.
- According to the security zone division rules of gateway 1 and gateway 2, the zone connected to the internal network is the Trust zone, the zone connected to the external network is the Untrust zone, and the IP address of the device is the Local zone. The security policy configuration is as follows:
 - Security policy of gateway 1:
 - Local -> Untrust, IP address of gateway 1: X -> IP address of gateway 2: Z;
 - Trust -> Untrust, branch intranet address -> HQ intranet address;
 - Untrust -> Local, IP address of gateway 2: Z -> IP address of gateway 1: X.
 - Security policy of gateway 2:
 - Local -> Untrust, IP address of gateway 2: Z -> IP address of the NAT device: Y;
 - Trust -> Untrust: intranet IP address of the HQ -> intranet IP address of the branch;
 - Untrust -> Local, IP address of the NAT device: Y -> IP address of gateway 2: Z.

NAT Traversal Scenario (3/3)

- In this scenario, the NAT device is the management device of the branch. It provides the NAT Server function and maps the interface address of the gateway. IPsec is configured on the headquarter by manually specifying the peer. In this case, the headquarter can initiate ISAKMP negotiation and traffic access.



40 Huawei Confidential

HUAWEI

- In this scenario, the branch gateway is a firewall, the public IP address of the NAT device is fixed, and the headquarter knows the public IP address of the NAT device. Therefore, you can configure IPsec using a template or manually specify a peer. NAT Server is configured on the NAT device to map the IP: X of gateway 1 to the public network. Therefore, the headquarter can initiate ISAKMP negotiation to the branch.
- According to the security zone division rules of gateway 1 and gateway 2, the zone connected to the internal network is the Trust zone, the zone connected to the external network is the Untrust zone, and the IP address of the device is the Local zone. The security policy configuration is as follows:
 - Security policy of gateway 1:
 - Local -> Untrust, IP address of gateway 1: X -> IP address of gateway 2: Z;
 - Trust -> Untrust, branch intranet address -> HQ intranet address;
 - Untrust -> Local, IP address of gateway 2: Z -> IP address of gateway 1: X.
 - Security policy of gateway 2:
 - Local -> Untrust, IP address of gateway 2: Z -> IP address of the NAT device: Y;
 - Trust -> Untrust: intranet IP address of the HQ -> intranet IP address of the branch;
 - Untrust -> Local, IP address of the NAT device: Y -> IP address of gateway 2: Z.

Key Configuration in the NAT Traversal Scenario

- This command is used to enable NAT traversal.

```
<sysname> system-view  
[sysname] ike Peer Peer1  
[sysname-ike-Peer-Peer1] nat traversal
```

- When NAT traversal is configured, the IPsec proposal **ipsec proposal** must be ESP.

```
<sysname> system-view  
[sysname] ipsec proposal newprop1  
[sysname-ipsec-proposal-newprop1] transform esp
```

- Run the **ipsec nat-traversal source-port** command to set the UDP port number for IPsec NAT traversal. The default UDP port number is 4500.

```
<sysname> system-view  
[sysname] ipsec nat-traversal source-port 4510
```

- When a NAT gateway is deployed between peers, the device on the internal network of the NAT gateway sends NAT keepalive packets to the peer at a specified interval to prevent NAT entries from aging. This keeps the NAT session alive.

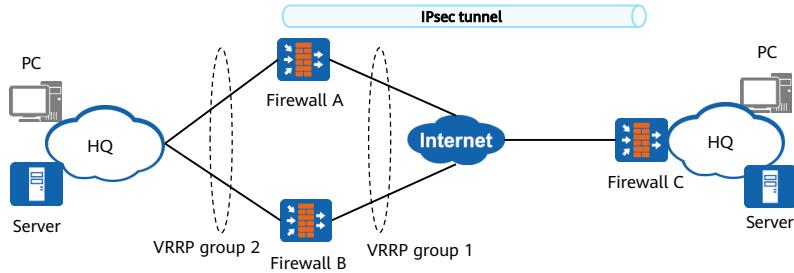
```
<sysname> system-view  
[sysname] ike nat-keepalive-timer interval 30
```

Contents

1. Basic Principles of IPsec VPN
2. Application Scenarios of IPsec VPN
3. **High Reliability of IPsec VPN**
 - Hot Standby
 - Link Redundancy
 - Intelligent Uplink Selection
4. Troubleshooting of IPsec VPN

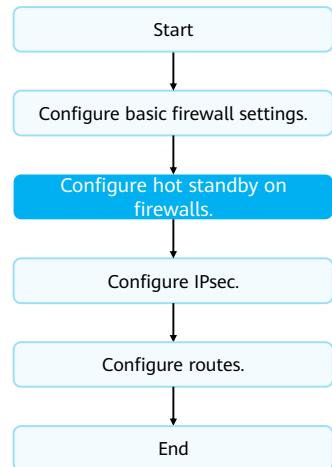
IPsec Hot Standby

- In the HQ-to-branch scenario, VRRP group 1 is configured on firewall A and B, and an IPsec tunnel is established between VRRP group 1 and the physical interface of the branch gateway firewall C. When the physical interface, link, or host of active firewall A is faulty, traffic is diverted to standby firewall B for forwarding. In this way, the original IPsec tunnel is not torn down, and the switchover speed is faster.



Configuration Roadmap

- Complete basic firewall settings, such as adding security zones and related policies to interfaces.
- Configure two firewalls to work in active/standby mode.
- Configure basic IPsec parameters, including the remote and local information, and select interesting data flows and security proposals.
- Configure routes to ensure interconnection.



Key Configuration (1/2)

- Assume that the heartbeat interfaces of the two firewalls are GE0/0/3, and the uplink and downlink interfaces are GE0/0/2 and GE0/0/4. The key configuration of hot standby are as follows:

VRID	Interface	Interface IP Address/Mask	Virtual IP Address/Mask	Virtual MAC	Edit
2	GE0/0/2	40.1.1.124	1.1.1.124	Disabled	<input type="checkbox"/>
1	GE0/0/4	10.20.1.124	10.20.1.254/24	Disabled	<input type="checkbox"/>

45 Huawei Confidential



Key Configuration (2/2)

- Assume that two firewalls are connected to the Internet through GE0/0/2 and VRRP group 2 consists of these two interfaces. Key IPsec configurations at the HQ are as follows:

Add IPSec Policy

Scenario: Site-to-site (selected) / Site-to-multisite

Option: IPSec Intelligent Link Selection

Virtual System Configuration

Virtual System: public

Basic Configuration

Policy Name: map1
Local Interface: GE0/0/2
Local Address: 1.1.1.1
Peer Address: Any

Note: To ensure that negotiation messages interoperate, enable the two-way security policy.
[Add Security Policy]

Authentication Type: Pre-shared key
 Pre-shared key
Pre-shared key:

Local ID: IP Address: 1.1.1.1
Peer ID: Any

Add IPSec Policy

Scenario: Site-to-site (selected) / Site-to-multisite

Option: IPSec Intelligent Link Selection

Virtual System Configuration

Virtual System: public

Basic Configuration

Policy Name: map1
Local Interface: GE0/0/1
Local Address: 1.1.1.1
Peer Address: Any

Note: To ensure that negotiation messages interoperate, enable the two-way security policy.
[Add Security Policy]

Authentication Type: Pre-shared key
 Pre-shared key
Pre-shared key:

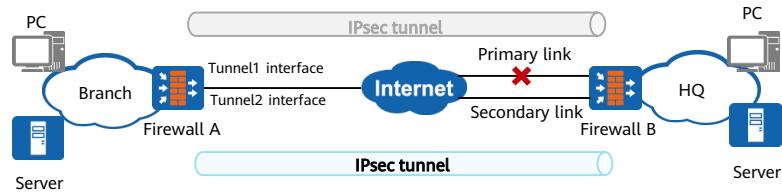
Local ID: IP Address:
Peer ID: Any

Contents

1. Basic Principles of IPsec VPN
2. Application Scenarios of IPsec VPN
3. **High Reliability of IPsec VPN**
 - Hot Standby
 - Link Redundancy
 - Intelligent Uplink Selection
4. Troubleshooting of IPsec VPN

IPsec Primary/Secondary Link Redundancy

- To improve network reliability, an enterprise branch establishes an IPsec connection with the enterprise headquarter through two links in active/standby mode. When the primary link is faulty, the secondary link is used to establish an IPsec tunnel. The old IPsec tunnel is torn down, and traffic switchover is complete.
- As shown in the following figure, firewall A connects to firewall B through two active and secondary links. Normally, traffic is transmitted through the IPsec tunnel established between the primary link and Tunnel1. When the primary link fails, firewall A uses Tunnel2 to establish an IPsec tunnel with the secondary link of firewall B.



Key Configuration (1/2)

- The active egress of the headquarter firewall is GE0/0/1, and the standby egress is GE0/0/2. You need to create two sets of IPsec policies.

```
[FW_B] ipsec policy map1 10 isakmp  
[FW_B-ipsec-policy-isakmp-map1-10] security acl 3000  
[FW_B-ipsec-policy-isakmp-map1-10] proposal tran1  
[FW_B-ipsec-policy-isakmp-map1-10] ike-Peer b  
[FW_B-ipsec-policy-isakmp-map1-10] quit
```

```
[FW_B] ipsec policy map2 10 isakmp  
[FW_B-ipsec-policy-isakmp-map1-10] security acl 3000  
[FW_B-ipsec-policy-isakmp-map1-10] proposal tran1  
[FW_B-ipsec-policy-isakmp-map1-10] ike-Peer b  
[FW_B-ipsec-policy-isakmp-map1-10] quit
```

- Invoked to two outbound interfaces respectively.

```
[FW_B] interface GigabitEthernet 0/0/1  
[FW_B-GigabitEthernet0/0/1] ipsec policy map1  
[FW_B-GigabitEthernet0/0/1] quit  
[FW_B] interface GigabitEthernet 0/0/2  
[FW_B-GigabitEthernet0/0/2] ipsec policy map2  
[FW_B-GigabitEthernet0/0/2] quit
```

Key Configuration (2/2)

- Create two tunnel interfaces on the branch firewall, borrow the IP address of the same physical interface, and apply different IPsec policies to the tunnel interfaces.

```
[FW_A] interface tunnel 1  
[FW_A-Tunnel1] ip address unnumbered interface GigabitEthernet 0/0/1  
[FW_A-Tunnel1] tunnel-protocol ipsec  
[FW_A-Tunnel1] quit
```

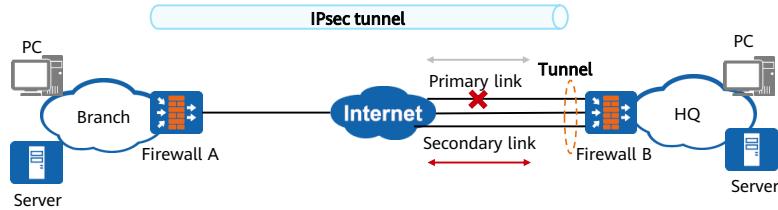
```
[FW_A] interface tunnel 2  
[FW_A-Tunnel1] ip address unnumbered interface GigabitEthernet 0/0/1  
[FW_A-Tunnel1] tunnel-protocol ipsec  
[FW_A-Tunnel1] quit
```

- Invoked to two outbound interfaces respectively.

```
[FW_A] interface tunnel 1  
[FW_A-Tunnel1] ipsec policy map1  
[FW_A-Tunnel1] quit  
[FW_A] interface tunnel 2  
[FW_A-Tunnel2] ipsec policy map2  
[FW_A-Tunnel2] quit
```

IPsec Multi-Link Redundancy

- To improve network reliability, an enterprise branch establishes an IPsec connection with the headquarter through two or more links. If the primary link fails, traffic is switched to the secondary link. IPsec tunnels do not need to be renegotiated, and traffic can be quickly switched.
- As shown in the following figure, firewall A connects to firewall B through two primary and secondary links. The system establishes an IPsec tunnel between the physical interface of firewall A and the tunnel interface of firewall B. Traffic is processed by IPsec through the tunnel interface and then sent through a physical interface selected from the routing table. If the primary link fails, traffic is switched to the secondary link.



Key Configuration

- A tunnel interface is created on the HQ device to establish an IPsec VPN with the branch. When the primary link fails, the route of the primary link becomes invalid, and traffic is switched to the secondary link. During the primary/secondary link switchover, IPsec traffic is not interrupted.

```
[FW_B] interface tunnel 0
[FW_B-tunnel0] tunnel-protocol ipsec
[FW_B-tunnel0] ip address 1.1.0.2 24
[FW_B-tunnel0] ipsec policy map1
[FW_B-tunnel0] quit
```

- Configure a static route to the branch. Assume that the IP address of the branch is 10.4.0.0/24.

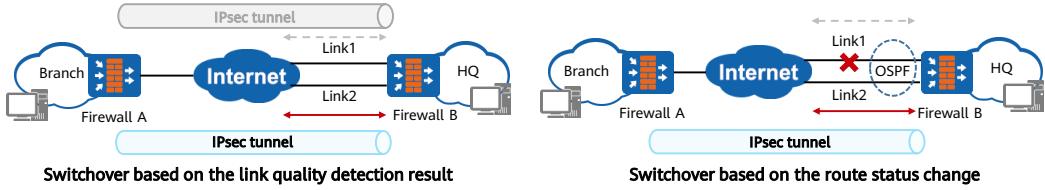
```
[FW_B] ip route-static 10.4.0.0 255.255.255.0 tunnel 0
```

Contents

1. Basic Principles of IPsec VPN
2. Application Scenarios of IPsec VPN
3. **High Reliability of IPsec VPN**
 - Hot Standby
 - Link Redundancy
 - Intelligent Uplink Selection
4. Troubleshooting of IPsec VPN

Intelligent Uplink Selection

- When the firewall functions as the gateway of a branch, you can configure IPsec intelligent uplink selection to implement dynamic switchover between multiple IPsec tunnels. The IPsec intelligent uplink selection function can be used in two scenarios based on the link switchover mechanism. One is to switch the link based on the link quality detection result, and the other is to switch the link based on the route status change.
 - Based on the link quality detection result: The firewall detects the latency or packet loss rate of the current IPsec tunnel in real time. When the latency or packet loss rate is higher than the preset threshold, the firewall dynamically switches to the secondary link to establish another IPsec tunnel.
 - Based on the route status change: An IPsec tunnel is established based on the route status. If the link is faulty and the route is unreachable, the IPsec tunnel is automatically switched to the secondary link.



54 Huawei Confidential

HUAWEI

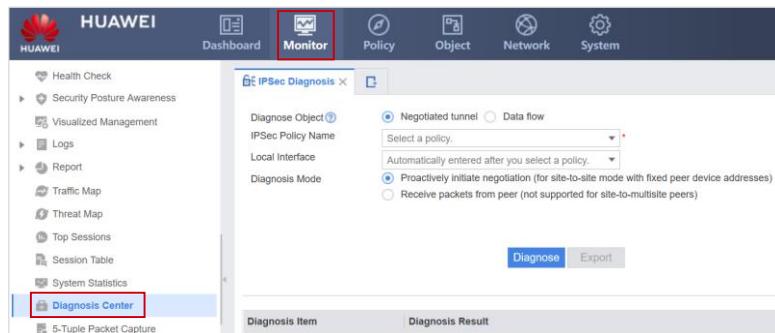
- Switchover based on the link quality detection result: After IPsec intelligent uplink selection is configured on firewall B, firewall B selects a link to establish an IPsec tunnel (Link1). Then, firewall B sends ICMP packets to detect the latency or packet loss rate of the IPsec tunnel. When the latency or packet loss rate of the tunnel is higher than the preset threshold, firewall B tears down the current IPsec tunnel and selects another link to establish an IPsec tunnel (Link2). In this way, the branch and headquarter can always use the IPsec tunnel that meets the quality requirements for communication.
- Switchover based on the route status change: There are two links (Link1 and Link2) from the branch firewall A to the headquarter firewall B. A dynamic routing protocol (OSPF is used as an example) runs between firewall B and the Internet. Configure IPsec intelligent uplink selection on firewall B to implement dynamic switchover between multiple IPsec tunnels between the branch and headquarter. If both Link1 and Link2 are normal, firewall B selects a link to establish an IPsec tunnel. For example, Link1 is selected. When Link1 is faulty, the route to firewall A through Link1 disappears. Firewall B automatically switches the IPsec tunnel to Link2 based on the route change.

Contents

1. Basic Principles of IPsec VPN
2. Application Scenarios of IPsec VPN
3. High Reliability of IPsec VPN
- 4. Troubleshooting of IPsec VPN**

IPsec Diagnosis – Web UI

- You can apply the following method for IPsec accessing failure.
 - Choose **Monitor > Diagnosis Center** and click **IPsec Diagnosis**.
 - Configure IPsec diagnosis, including the diagnosis object, IPsec policy name, local interface, and policy name. Click **Diagnose** to obtain the diagnostic information.



IPsec Diagnosis - CLI

- Check statistics about IPsec packets, such as statistics about incoming and outgoing packets with security protection enabled, statistics about encrypted and decrypted packets, detailed statistics about discarded packets under security protection, and statistics about packets related to IKE negotiation. The information helps diagnose IPsec faults.

```
<sysname> display ipsec statistics
```

- Check the IKE SA negotiation result.

- To view SA information, run the **display ike sa** command. The command output contains the SA connection index, remote IP address of the SA, VPN instance name, SA phase, and SA status.

```
<sysname> display ike sa
```

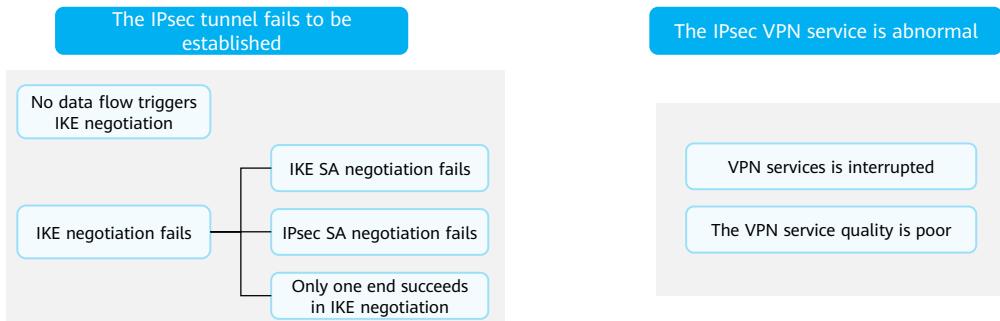
- Check the IPsec SA configuration.

```
<sysname> display ipsec sa
```

- Description of the **display ipsec statistics** command output
 - **IPsec statistics information:** IPsec packet statistics.
 - **Number of IPsec tunnels:** Number of IPsec tunnels.
 - **Number of standby IPsec tunnels:** Number of standby IPsec tunnels when SPUs are backed up.
 - **the security packet statistics:** Statistics about packets protected.
 - **input/output security packets:** Number of incoming and outgoing packets that are protected.
 - **input/output security bytes:** Number of incoming and outgoing bytes that are protected.
 - **input/output dropped security packets:** Number of discarded incoming and outgoing packets under protection.
 - **the encrypt packet statistics:** Statistics about encrypted packets.
 - **the decrypt packet statistics:** Statistics about decrypted packets.
 - **dropped security packet detail:** Detailed statistics about discarded security-protected packets.
 - **negotiate about packet statistics:** Statistics about packets related to IKE negotiation.

Major IPsec VPN Faults

- Based on the fault symptom, IPsec faults can be divided into the following types:
 - The IPsec tunnel fails to be established (tunnel negotiation fails).
 - The service is abnormal after the IPsec tunnel is successfully established (encrypted data flows fail to be forwarded).



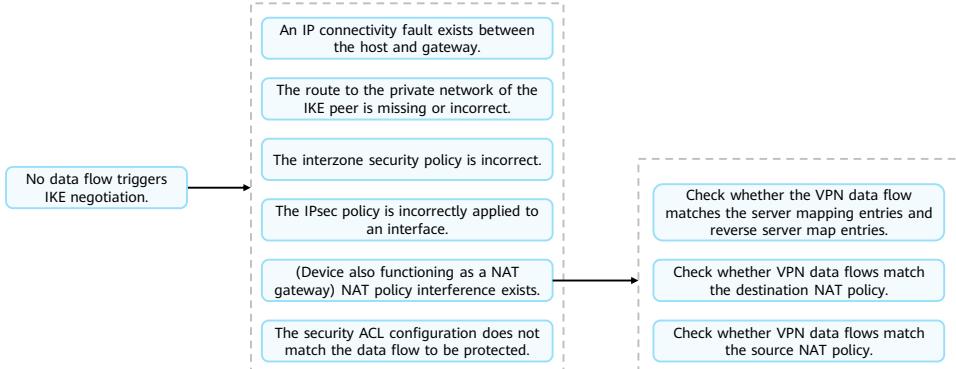
58 Huawei Confidential

HUAWEI

- You can troubleshoot IPsec faults based on the stage during which a fault occurs.
 - During configuration stage, the IPsec configuration page or commands are unavailable.
 - In the negotiation triggering stage, no data flow triggers IKE negotiation.
 - In the IKE negotiation stage, the IKE negotiation fails (IKE SA or IPsec SA negotiation fails).
 - In the data transmission stage, the IKE negotiation succeeds, but the VPN service is abnormal (disconnected or of a poor quality).
- Most IPsec faults occur in IKE negotiation. Therefore, analyze the IKE negotiation process for troubleshooting. Other faults are usually caused by incorrect configuration of basic firewall features, such as the license, interface, link, routing, security zone, and NAT configurations. Analyze these faults based on the specific scenarios.

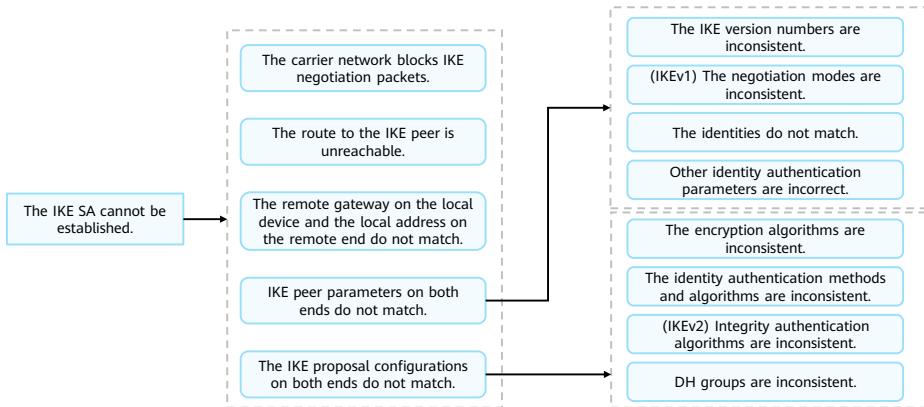
IPsec VPN Troubleshooting Roadmap - No Data Flow Triggers IKE Negotiation

- If IKE negotiation fails to be established, check whether data flows trigger IKE negotiation first. The possible causes and check measures are as follows:



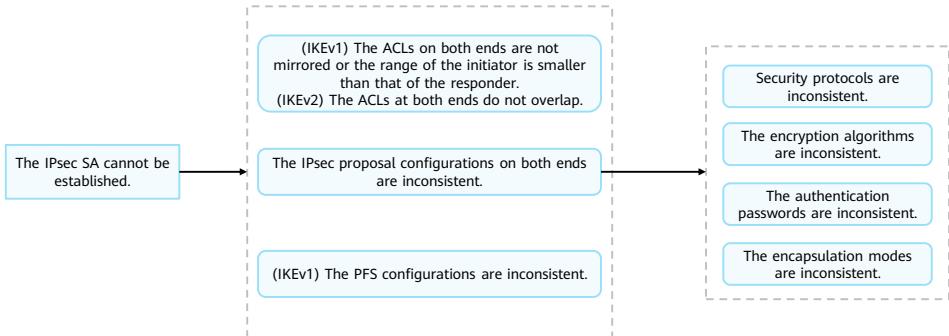
IPsec VPN Troubleshooting Roadmap - IKE SA Negotiation Fails

- Data flows trigger IKE negotiation, but IKE negotiation fails. The possible causes are as follows:



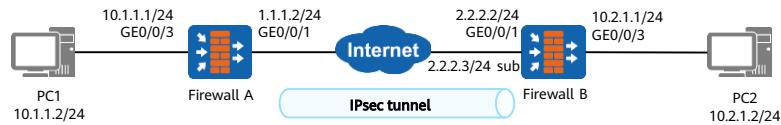
IPsec VPN Troubleshooting Roadmap - IPsec SA Negotiation Fails

- After IKE negotiation succeeds, the IPsec SA cannot be established. The possible causes are as follows:



Case 1: Fault Symptom

- An IPsec tunnel is established between two firewalls. The following figure shows that before the parameters are modified, the tunnel can be established successfully. However, after a sub-address is added to the public network interface of firewall B and the IPsec configuration is modified, the tunnel fails to be established. The check result shows that IPsec and IKE parameters of both ends, routes, interfaces, and security policies are correctly configured.



- To connect an interface on a routing device to multiple subnets, you can configure multiple IP addresses for the interface, one as the primary IP address and others as secondary IP addresses. The sub-address is the secondary IP address of the interface.

Case 1: Fault Analysis

- Run the **display ike sa** command to check whether the IKE SA exists on firewall A. The command output shows that the **sa number** has changed to 0.

```
<FW_A> display ike sa  
current ike sa number: 0
```

- Run the **display ike peer** command to check the IKE peer configurations on the firewall A. The remote address of firewall A is 2.2.2.2.

```
[FW_A] display ike peer brief  
current ike Peer number: 1  
-----  
Peer Name Version Exchange-mode Proposal Id-type RemoteAddr  
-----  
b v1v2 N/A 10 IP 2.2.2.2
```

- Query the configuration on the firewall B. It is found that the remote address of firewall A is different from the local address of firewall B.

```
[FW_B-ipsec-policy-isakmp-map1-10]display this  
#  
ipsec policy map1 10 isakmp  
security acl 3000  
ike-Peer a  
proposal tran1  
local-address 2.2.2.3
```

- Analyze the routes between IKE peers, IKE peers, and IKE proposals. The fault is caused by the addition of a sub-address to the public network interface of firewall B. It is suspected that the sub-address triggers IPsec negotiation, leading to the IKE negotiation failure.

Case 1: Troubleshooting

- The IKE negotiation fails because the remote gateway address of the local end does not match the local address of the remote end. Therefore, you only need to change the remote address of the IKE peer on firewall A.

```
[FW_A] ike Peer b  
[FW_A-ike-Peer-b] remote-address 2.2.2.3  
[FW_A-ike-Peer-b] quit
```

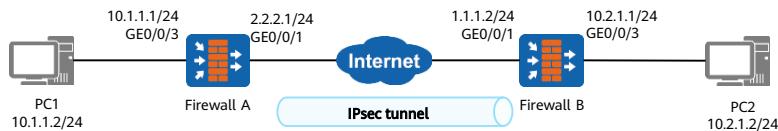
- Ping the private networks at both ends again. The ping operation succeeds. Check the IKE SA and find it is re-established.

```
[FW_A] display ike sa  
current ike sa number: 2  
-----  
conn-id  Peer      flag    phase  vpn  
-----  
40003   2.2.2.3  RD|ST   v2:2  public  
3        2.2.2.3  RD|ST   v2:1  public
```

- Summary: When you configure an IPsec policy, the **local-address** command is optional. If the IP address used by the local end to initiate IPsec tunnel negotiation is different from the IP address of the interface to which the IPsec policy is applied, set **local-address** to the IP address used by the local end to initiate IPsec tunnel negotiation. This IP address must be the same as the destination IP address configured using the **remote-address** command on the remote end.

Case 2: Fault Symptom

- A site-to-site IPsec VPN is established between firewall A and firewall B. After the configuration is complete, the following situations occur:
 - Ping PC2 from PC1. The ping operation fails. The IPsec VPN is not established.
 - Ping GE0/0/3 of firewall A from PC2. The ping operation succeeds, and a tunnel is established.
 - The IP address and gateway configurations on the PCs are correct, the IP address, route, security zone, and interzone policy configurations on the firewall A and firewall B are correct.



Case 2: Fault Analysis (1/2)

- When PC2 can ping PC1, run the **display ike sa** and **display ipsec sa** commands. The IKE SA and IPsec SA can be established between firewall A and firewall B.

[FW_A] **display ike sa**

current ike sa number: 2

conn-id	Peer	flag	phase	vpn
40050	1.1.1.2	RD ST	v1:2	public
40049	1.1.1.2	RD ST	v1:1	public

[FW_B] **display ike sa**

current ike sa number: 2

conn-id	Peer	flag	phase	vpn
40050	2.2.2.1	RD ST	v1:2	public
40049	2.2.2.1	RD ST	v1:1	public

[FW_A] **display ipsec sa**

ipsec sa information:

=====

Interface: GigabitEthernet0/0/1

=====

IPSec policy name: "pc1"

Sequence number : 1

Acl group : 3000/IPv4

Acl rule : 5

Mode : isakmp

=====

Connection ID : 67108879

Encapsulation mode: Tunnel

Failover state : Master

[FW_B] **display ipsec sa**

ipsec sa information:

=====

Interface: GigabitEthernet0/0/1

=====

IPSec policy name: "pc2"

Sequence number : 1

Acl group : 3000/IPv4

Acl rule : 5

Mode : isakmp

=====

Connection ID : 67108879

Encapsulation mode: Tunnel

Failover state : Master

- Basic configurations, such as the IP address, route, and interzone policy, are correctly configured. After the **display ike sa** and **display ipsec sa** commands are run, the SA is normal. Then, continue to check other problems.

Case 2: Fault Analysis (2/2)

- Run the **display acl** command. The command output shows that the ACL rule range is incorrect.

```
[FW_A] display acl 3000  
Acl's step is 5  
rule 5 permit ip source 10.1.1.1 0.0.0.0 destination 10.2.1.0 0.255.255.255
```

```
[FW_B] display acl 3000  
Acl's step is 5  
rule 5 permit ip source 10.2.1.0 0.255.255.255 destination 10.1.1.1 0.0.0.0
```

- Check the possible causes in IKEv1 and IKEv2. Run the **display acl** command. The command output shows that the ACL rules on both ends do not contain the IP address of PC1. Therefore, the problem is caused by the ACL interesting traffic failure.

Case 2: Troubleshooting and Summary

- The ACL rules configured on firewall A and firewall B do not contain the IP address of PC1. As a result, the service fails when PC1 pings PC2. The fault is rectified after the ACL rules on the firewall are modified.

```
[FW_A-acl-adv-3000] rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.2.1.0 0.255.255.255  
Warning: The rule already exists. Are you sure to update? [Y/N]y
```

```
[FW_B-acl-adv-3000] rule 5 permit ip source 10.2.1.0 0.255.255.255 destination 10.1.1.0 0.0.0.255  
Warning: The rule already exists. Are you sure to update? [Y/N]y
```

- IPsec uses advanced ACLs to define the data flows to be protected. You are advised to check whether the ACL rules at both ends of the tunnel completely contain the data flows to be protected and ensure that the ACL rules at both ends of the tunnel are mirrored.

- Mirroring on both ends of a tunnel is not a prerequisite. IKEv1 requires that ACL rules configured on both ends mirror each other or the ACL rules configured on the initiator are included in those of the responder. In IKEv2 negotiation, the two ends use overlapping address ranges as the negotiation result.
- In actual configuration, you are advised to configure mutual mirroring for ACL rules at both ends of a tunnel, which is simple and error-prone.

Quiz

1. (Multiple-answer question) According to the packet encapsulation mode, which of the following IPsec encapsulation modes can be used? ()
 - A. Transport mode
 - B. Tunnel mode
 - C. Main mode
 - D. Fast mode

1. AB

Summary

- This course describes the background, basic concepts, key protocols, application scenarios, and reliability technologies of IPsec VPN. In addition, this course describes the basic IPsec configuration roadmap and troubleshooting roadmap.
- Upon completion of this course, you will have an in-depth understanding of IPsec VPN applications and be able to independently configure IPsec VPN.

Recommendations

- Huawei official websites:
 - Enterprise service: <https://e.huawei.com/en/>
 - Technical support: <https://support.huawei.com/enterprise/en/index.html>
 - Online learning: <https://www.huawei.com/en/learning>

Acronyms and Abbreviations (1/3)

Acronym/Abbreviation	Full Name
3DES	Triple Data Encryption Standard
ACL	Access Control List
AES	Advanced Encryption Standard
AH	Authentication Header
CA	Certification Authority
DES	Data Encryption Standard
DH	Diffie-Hellman
DPD	Dead Peer Detection
ESP	Encapsulating Security Payload
GCM	Galois/Counter Mode

Acronyms and Abbreviations (2/3)

Acronym/Abbreviation	Full Name
GMAC	Galois Message Authentication Code
GRE	Generic Routing Encapsulation
IKE	Internet Key Exchange
IPsec	Internet Protocol Security
ISAKMP	Internet Security Association and Key Management Protocol
IS-IS	Intermediate System-to-Intermediate System
MD5	Message Digest 5
NAPT	Network Address and Port Translation
NAT	Network Address Translation
OSPF	Open Shortest Path First

Acronyms and Abbreviations (3/3)

Acronym/Abbreviation	Full Name
PKI	Public Key Infrastructure
PRF	Pseudorandom Function
RSA	Rivest, Shamir, and Adleman
SA	Security Association
SHA1	Secure Hash Algorithm 1
SHA2	Secure Hash Algorithm 2
SHA3	Secure Hash Algorithm 3
SNAT	Source Network Address Translation
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。
Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

Copyright©2022 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product performance, market position, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.



SSL VPN Technology and Application



Foreword

- With the development of the era, remote office has gradually become a trend. This office mode also means that enterprises need to rely on the public network lines provided by the ISP to establish dedicated communication tunnels, and then provide reliable and secure data transmission for users. Mobile users use the SSL VPN technology to remotely access the network for work. It is secure and convenient for mobile users to access intranet resources and improve work efficiency.
- This course describes SSL VPN application scenarios and SSL VPN troubleshooting roadmap.

Objectives

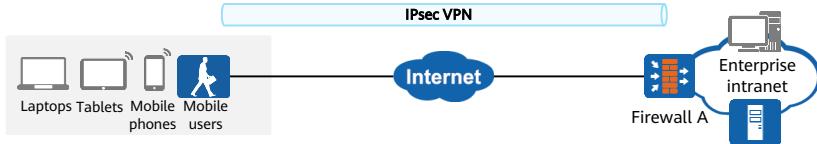
- On completion of this course, you will be able to:
 - Understand application scenarios of SSL VPN.
 - Master the main functions and principles of SSL VPN.
 - Understand the SSL VPN networking.
 - Master the configuration of SSL VPN.

Contents

- 1. Overview of SSL VPN**
 - Background of SSL VPN
 - Basic Principles of SSL VPN
2. Service Functions of SSL VPN
3. Examples for Configuring the SSL VPN
4. SSL VPN Troubleshooting

Disadvantages of IPsec VPN

- With the development of the era, mobile users gradually need to access the intranet. In business trip scenarios, employees need to use devices such as laptops to securely access internal resources of the enterprise. The IPsec VPN technology first emerges to meet this requirement.



- However, IPsec VPN has the following disadvantages:

High usage threshold

When using the client for the first time, a common user needs to set many encryption connection parameters.

High O&M cost

Professional technical personnel are responsible for obtaining, installing, and upgrading the IPsec client software.

Coarse-grained access permission management

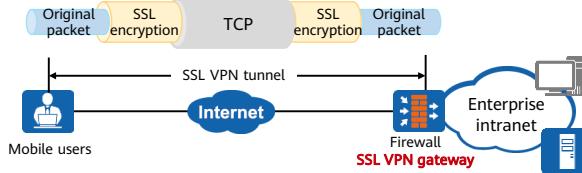
Access is controlled based on 5-tuple.

Supported by limited endpoints

PCs are well supported, but new devices such as mobile phones and tablets are not fully supported.

Overview of SSL VPN

- SSL VPN can solve the problems of IPsec VPN in remote access.
- SSL VPN is a VPN technology that uses the SSL/TLS protocol to implement secure remote access. It is mainly used to ensure that mobile users can securely and efficiently access internal network resources outside an enterprise.

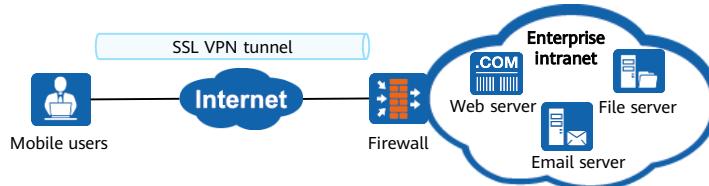


- Compared with IPsec VPN, SSL VPN has the following characteristics:

Low usage threshold	Simple O&M	Fine-grained access permission management	Supported by multiple endpoints
Users only need to open the website in the browser and enter the user name and password to access intranet resources or download the client.	Users can download and install the client by using a browser, reducing the pressure of maintaining the client.	Parses protocols in the application layer, associates user roles, and implements fine-grained access control for users.	Supports access from various endpoints, such as mobile phones and tablets, and is applicable to business trips and remote office scenarios.

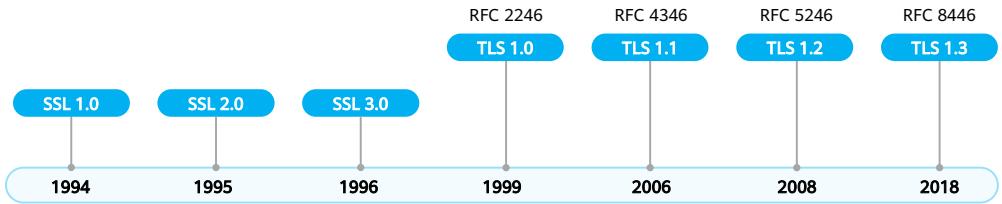
Application Scenarios of SSL VPN

- As a new lightweight remote access solution, SSL VPN applies to scenarios where employees need to remotely access enterprise internal resources during business trips. In addition, SSL VPN implements refined control on users' permissions to access intranet resources.
- The firewall, as the enterprise egress gateway, connects to the Internet and provides SSL VPN access services for mobile users. After a mobile user uses an endpoint (such as a laptop, tablet, or smart phone) to establish an SSL VPN tunnel with the firewall, users can use the SSL VPN tunnel to remotely access intranet resources, such as the web server, file server, and mail server.



Development History of SSL/TLS

- The SSL is a network security protocol first launched by Netscape in 1994 to protect web communication. It works over TCP and is mainly used to encrypt and decrypt HTTP (HTTPS).
- In 1999, Netscape submitted the SSL to the IETF. After standardizing the SSL, the IETF named it the Transport Layer Security (TLS). The implementation principle of TLS is basically the same as that of SSL.
- The SSL has three versions, but all of them have serious security vulnerabilities. Currently, it has been disabled and eliminated by most vendors. TLS has gradually become the mainstream protocol for encrypting HTTP traffic and has undergone multiple version iterations.



- Currently, the SSL VPN function of Huawei USG6000E series firewalls supports TLS 1.0, TLS 1.1, and TLS 1.2.

Comparison Between SSL VPN and IPsec VPN

- The following table compares SSL VPN and IPsec VPN in various aspects.

Requirements for Remote Access		SSL VPN	IPsec VPN
Security	Transmission encryption	Common algorithms	Common algorithms
	Identity authentication	Various types and high strength	Few types and low strength
	Permissions	Fine-grained	Coarse-grained
	Antivirus	Can be implemented	Difficult to implement
Access	Access endpoint	Support various types of endpoints	Support a few types of endpoints
Usage	Client installation	Installation-free or automatic installation	Pre-installation
	Client maintenance	Automatic configuration	Manual configuration
Identity authentication integration and application bearing	Identity authentication integration	Support various authentication types and is easy to integrate with the original identity authentication system	Support a few authentication types and is difficult to integrate with the original identity authentication system
	Application bearing	Support various IP applications	Only support IP unicast applications

- Antivirus:

- After the ActiveX plug-in or client is installed on the SSL VPN, user's endpoint security can be checked to prevent endpoints intruded by viruses from accessing the VPN. However, IPsec cannot implement this function.

- Identity authentication integration:

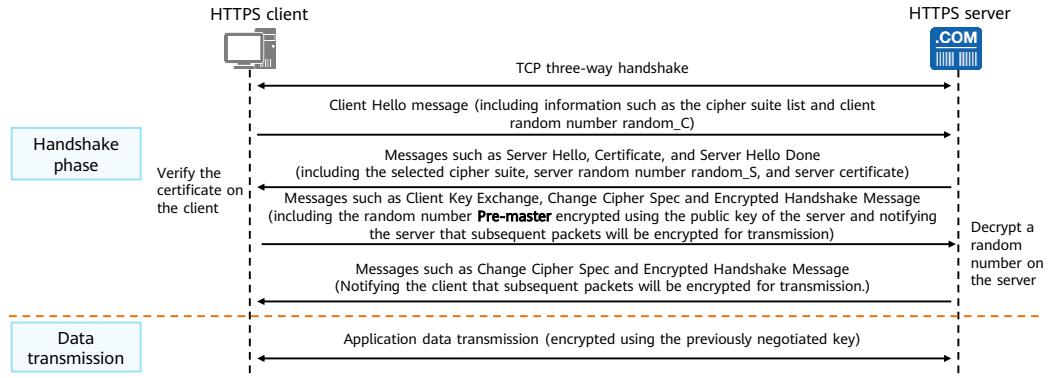
- IPsec VPN supports only common algorithm authentication and cannot use two-factor authentication or AD domain authentication. If an AD domain controller exists in the enterprise's internal system, the new IPsec VPN cannot be associated with the original AD domain controller identity authentication, thereby wasting resources.
 - SSL VPN supports local authentication, server authentication, certificate anonymous authentication, and certificate challenge authentication. If an AD domain controller exists in the enterprise's internal system, the new SSL VPN can be associated with the original AD domain controller identity authentication, thereby facilitating integration.

Contents

- 1. Overview of SSL VPN**
 - Background of SSL VPN
 - Basic Principles of SSL VPN
2. Service Functions of SSL VPN
3. Examples for Configuring the SSL VPN
4. SSL VPN Troubleshooting

Encryption and Decryption Principles of TLS

- HTTP traffic encryption in SSL VPN is implemented based on the TLS. The TLS can establish a secure data transmission channel. The establishment process can be divided into two phases: handshake phase and data transmission phase. The working principle is as follows:



- The key used for data encryption is calculated based on the following three parameters: random_C on the client, random_S on the server, and Pre-master.
- The random number **Pre-master** is generated by the client, and sent to the server after being encrypted using the public key in the server certificate. The server decrypts the random number using the private key to obtain the random number **Pre-master**. The private key of the server is confidential. Therefore, the third party cannot decrypt the private key, thereby ensuring that the finally calculated key is secure.
- The symmetric key encryption algorithm is used to transmit application data, which is efficient.

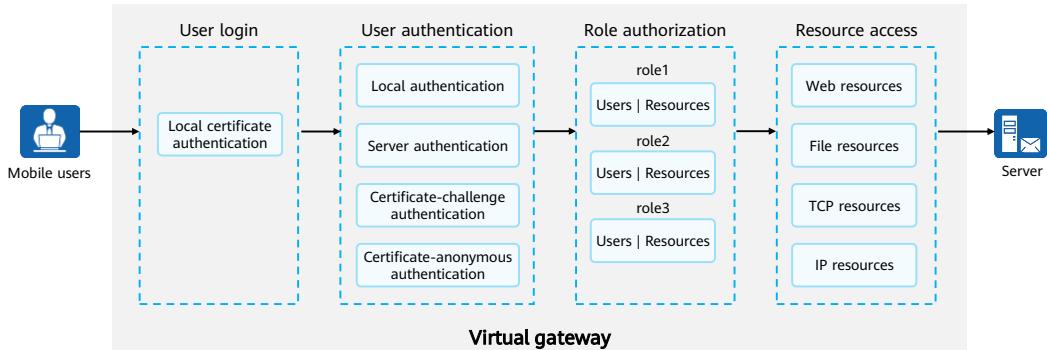
Service Functions of SSL VPN

- To implement fine-grained control over the resource access permissions for mobile users, SSL VPN classifies intranet resources into web resources, file resources, port resources, and IP resources. Each type of resource has a corresponding access mode. The following table lists the resource access modes.

SSL VPN Service	Description
Web proxy	Mobile users access intranet web resources through the web proxy service.
File sharing	Mobile users access the intranet file server (running the SMB-capable Windows OS or NFS-capable Linux OS) using the file sharing service. Mobile users can use web browsers to create and view folders as well as upload, download, rename, and delete files, just as they do on local file systems.
Port forwarding	Mobile users access intranet TCP resources through the port forwarding service. Port forwarding applies to TCP services, such as Telnet, remote desktop, FTP, and email. It is a port-level security mechanism for accessing resources on an intranet from the Internet.
Network extension	Mobile users access intranet IP resources through the network extension service. IP resources include web, file, and TCP resources. The network extension service is enabled when network resource types are not distinguished.

SSL VPN Virtual Gateway

- The firewall provides SSL VPN access services for mobile users through virtual gateways, which offer a unified portal for such employees to access enterprise intranet resources. The following figure shows how a mobile employee logs in to the SSL VPN virtual gateway and accesses intranet resources.



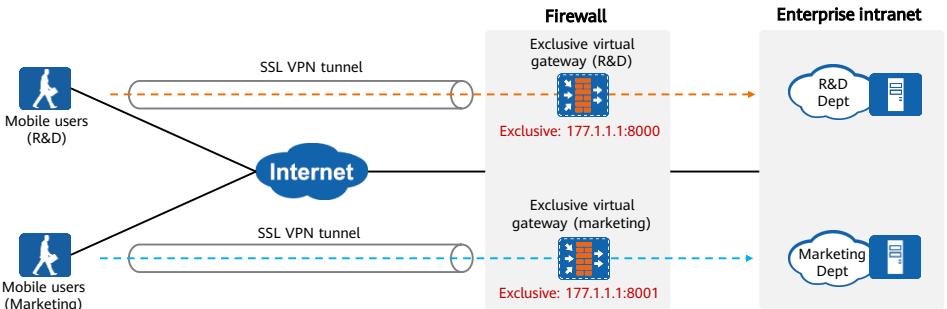
13 Huawei Confidential

 HUAWEI

- The process for a mobile employee to log in to the SSL VPN virtual gateway and access intranet resources is as follows:
 - User login: A mobile employee enters the IP address or domain name of the SSL VPN virtual gateway in the browser to request for establishing an SSL connection. The virtual gateway sends its certificate to the mobile user so that the user can authenticate the gateway. After the authentication succeeds, the mobile user establishes an SSL connection with the virtual gateway, and the virtual gateway login page is displayed.
 - User authentication: After you enter the user name and password on the login page, the virtual gateway authenticates the user. The virtual gateway can authenticate users in multiple modes, including local authentication, server authentication, certificate anonymous authentication, and certificate challenge authentication.
 - Role authorization: After user authentication succeeds, the virtual gateway checks the role of the user and pushes the resource links accessible to that role. A role represents the resource access permission of a type of users. For example, the resource access permission of a general manager role in an enterprise is different from that of a common employee role.
 - Resource access: The user clicks a link in the virtual gateway resource list to access the corresponding resource.
- Multiple virtual gateways can be created on one firewall and are independent of each other. Each virtual gateway is independently managed and has its own users and resources. A virtual gateway has no independent administrator. All the management operations such as creation, configuration, modification, and deletion of virtual gateways are performed by the system administrator of the firewall.

Virtual Gateway Type - Exclusive

- Virtual gateways are classified into exclusive virtual gateways and shared virtual gateways.
- An exclusive virtual gateway exclusively occupies a port of an IP address. Other virtual gateways cannot use this port but can use other ports of this IP address.
- Multiple exclusive virtual gateways can be configured in the public system or virtual system to isolate different service requirements. The application scenarios are as follows:



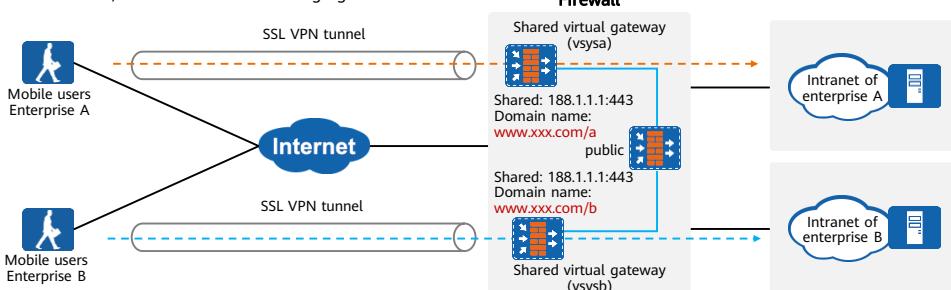
14 Huawei Confidential

 HUAWEI

- The preceding figure uses multiple exclusive gateways of the public system as an example. The functions of exclusive gateways of virtual systems are similar and are not described here.

Virtual Gateway Type - Shared

- The shared virtual gateway is usually used in the scenario where multiple virtual systems are configured on the firewall. The virtual gateways in multiple virtual systems provide SSL VPN services for mobile users by sharing the public IP address of the firewall. The public IP address and domain name must be preset in the public system of the firewall.
- Only one public IP address can be configured for the public system, and only one shared virtual gateway that uses this public IP address can be created for each virtual system.
- The shared virtual gateway uses the same IP address and port. Therefore, different access paths are required to distinguish different intranet resources, as shown in the following figure.

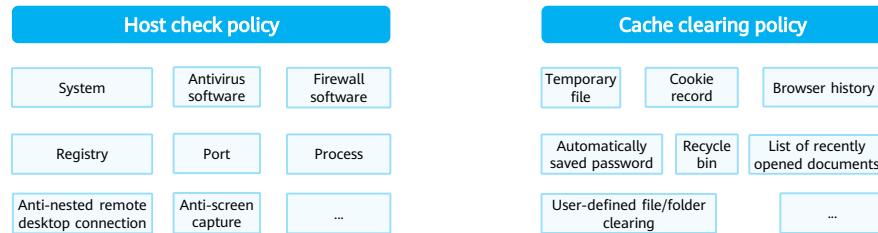


15 Huawei Confidential

- In the preceding figure, the public IP address is 188.1.1.1, and the corresponding domain name is www.xxx.com. This address and domain name must be preset in the public system of the firewall.

Endpoint Security

- Endpoint security is a method of checking whether endpoints are secure in SSL VPN. It prevents dangerous endpoints from accessing the intranet and prevents intranet resource information leakage. Endpoint security includes host check when a user attempts to log in to a virtual gateway and cache clearing after the user logs out from the virtual gateway.
 - When logging in to the virtual gateway, the user can access the SSL VPN only after the user endpoint passes the host check policy.
 - When a user host is disconnected from the SSL VPN, the endpoint security module can use the cache clearing policy to clear the access traces left on the endpoint during the user's access to the intranet, preventing intranet information leakage.



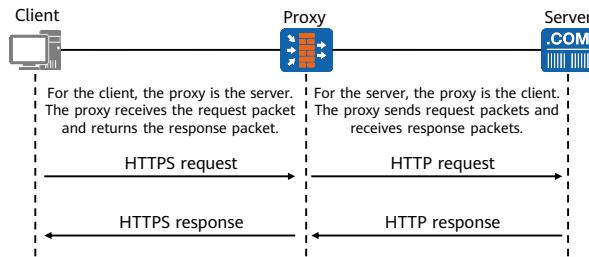
- The host check policy is used to check whether the host used for accessing a virtual gateway meets security requirements, check the operating system, port, process, antivirus software, firewall software, registry, and check whether specified files exist. The following functions are also provided:
 - Anti-nested remote desktop connection: This function checks whether a client enables any remote sharing program to prevent the client from being remotely controlled by other PCs.
 - Anti-screen capture: This function checks whether any screenshot program is running on a client to prevent information leaks.
- Cache clearing policies are used to clear the access history to enhance information security. The functions include:
 - Clearing the temporary files, automatically-saved passwords, cookies, browsing histories, recycle bin, and the lists of recently opened files.
 - Disabling autocomplete for the address bar and forms of the Internet Explorer.
 - Customizing the deletion of specific files, folders, etc.

Contents

1. Overview of SSL VPN
2. **Service Functions of SSL VPN**
 - Web Proxy
 - File Sharing
 - Port Forwarding
 - Network Extension
3. Examples for Configuring the SSL VPN
4. SSL VPN Troubleshooting

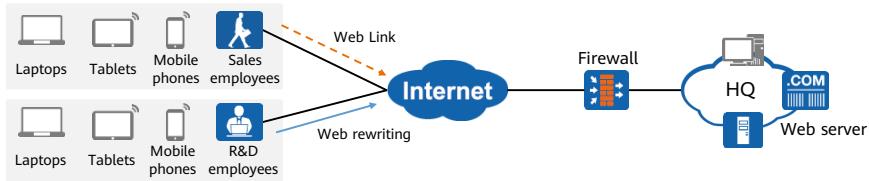
Overview of Web Proxy

- Web proxy is one of the SSL VPN functions. Users can use the firewall as a proxy to access intranet web server resources (URL resources). If necessary, the real URL of the intranet server can be hidden.
- The web proxy is implemented based on the HTTP proxy. The core of the web proxy is to forward requests, as shown in the following figure. Web proxy is classified into web rewriting and web link based on the implementation mode.



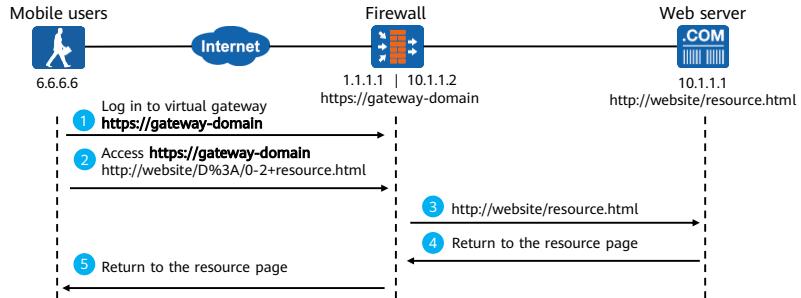
Application Scenario

- Generally, large- and medium-sized enterprises have complex network architectures and differentiated requirements. Mobile users have different requirements for accessing web applications at the HQ. Web proxy can be used to meet different requirements of employees.
- In this figure, we can see:
 - R&D mobile users need to use developed web UIs. For security purposes, the enterprise needs to hide the specific paths of these web UIs and adapt to employees' computers. The web rewriting mode can be used to rewrite the URL of the web UI for encrypting the link and adapting to the endpoint.
 - When sales employees visit customers, enterprises pay more attention to the efficiency of opening web links by sales employees. Problems such as image misplacement, inconsistent sizes, and incompatibility cannot occur. The web link mode can be used to directly forward web resource requests from sales employees without any processing, thereby avoiding image misplacement.



Interaction Procedure of Web Proxy Service

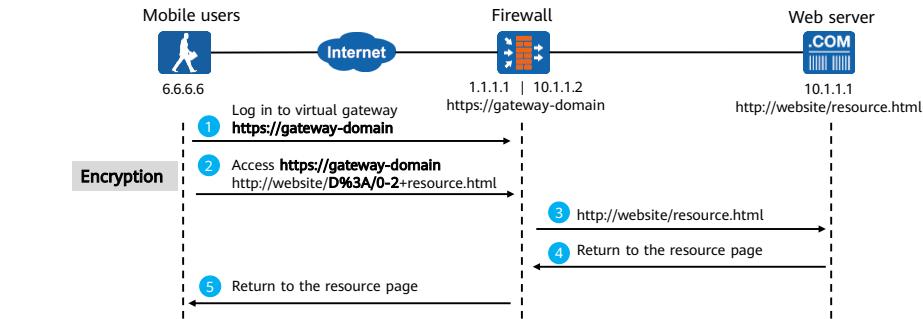
- The implementation principle of the web proxy function is that the process of accessing the web server by an Internet user is divided into two phases.
 - An HTTPS session is established between the Internet user and the virtual gateway of the firewall.
 - The virtual gateway of the firewall establishes an HTTP session with the web server.
- The firewall virtual gateway rewrites and forwards web requests when Internet users access the intranet web server.



- The following figure shows the service interaction process for a mobile user to access the intranet web server through the web proxy. The procedure is as follows:
 - The mobile user accesses the virtual gateway through the **https://gateway-domain**.
 - After logging in to the virtual gateway, the mobile user views a list of accessible web resources and clicks the link of the intended web resource. When the firewall presents the intranet resource (`http://website/resource.html`) to the mobile user, the firewall rewrites its URL. After the mobile user clicks the URL of the intended web resource, an HTTPS request is sent to the rewritten URL, which is the combination of the URL of the firewall (`https://svn`) and that of the intended web resource (`http://website/resource.html`).
 - After receiving the HTTPS request to the rewritten URL, the firewall initiates a new HTTP request to the actual URL of the intended web resource (`http://website/resource.html`).
 - The web server returns the resource page to the firewall through HTTP.
 - The virtual gateway forwards the resource page returned by the web server to the mobile user through HTTPS.

Web Rewriting

- Rewriting has two meanings:
 - Encryption: When a mobile user clicks a link in the resource list of the virtual gateway, the virtual gateway encrypts the actual URL that the user wants to access.
 - Adaption: These endpoints use various types of operating systems and browsers and they support different types of web resources. The virtual gateway rewrites web resources to adapt to different endpoints.



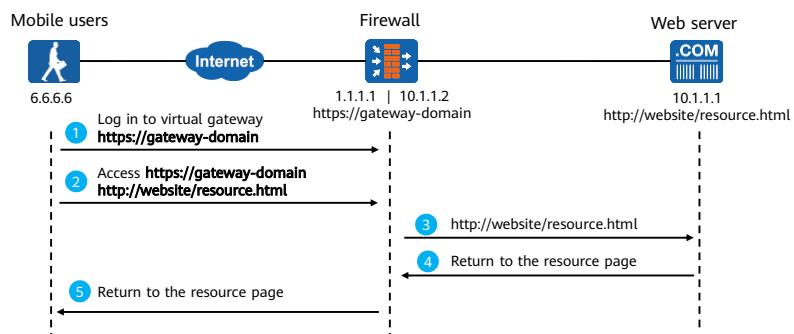
21 Huawei Confidential

HUAWEI

- Encryption: The step 2 in the figure shows that the actual URL of the intended web resource is <http://website/resource.html>. After web rewriting, the URL may be displayed as <http://website/D%3A/0-2+resource.html>. The rewritten URL is displayed instead of the actual URL so that the address of the web server on the enterprise network is hidden from outsiders. In web rewriting, the URL of the web resource page link object (such as Flash, PDF, and Java Applet) to be accessed is also encrypted.
- Adaptation: After the Web proxy function is enabled, the firewall automatically rewrites web resources. If the display of some HTML objects and ActiveX controls is still abnormal after the web proxy is enabled, administrators need to manually configure adaptation policies.

Web Link

- Web link does not encrypt or adapt to the original URL, but only forwards the web resource requests of mobile users. In steps 2 and 3 of the following figure, the URLs accessed by users remain unchanged. Therefore, the service processing efficiency of web link is higher than that of web rewriting.



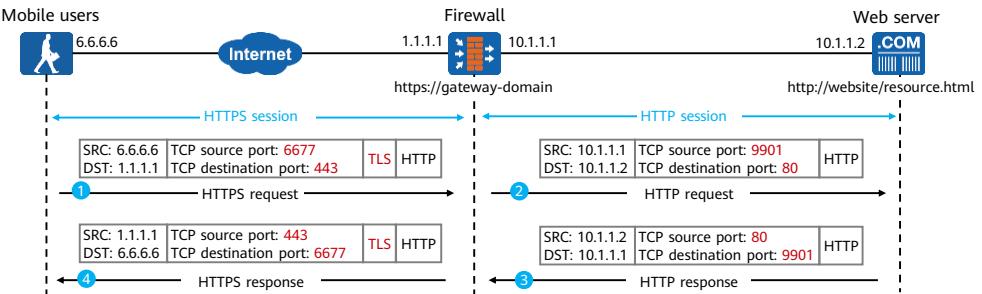
Comparison of Web Proxy Implementation Modes

- Web proxy can be implemented through web rewriting or web link. The following table lists the differences between web rewriting and web link.

Comparison Item	Web Rewriting	Web Link
Security	The real URL is rewritten and the intranet server address is hidden, which ensures high security.	The URL is not rewritten. Web requests and responses are directly forwarded, and the real address of the intranet server is exposed.
Usability	Do not depend on the Internet Explorer control and can be used in browsers in non-Internet Explorer environments.	Depend on the Internet Explorer control and cannot be used in a non-Internet Explorer environment.
Compatibility	Due to the rapid development of web technologies, the firewall cannot rewrite all types of URL resources. So, problems such as image misplacement and abnormal font display may occur.	Resources do not need to be rewritten. The firewall directly forwards requests and responses. Therefore, there is no page compatibility problem.
Suggestion	Web rewriting is recommended because it is the most secure and convenient access mode. If the page display is abnormal, consider the web link.	Web link is the best substitute for web rewriting. However, it depends on Internet Explorer controls and has limitations in use. In addition, intranet URLs are not rewritten, which poses security risks.

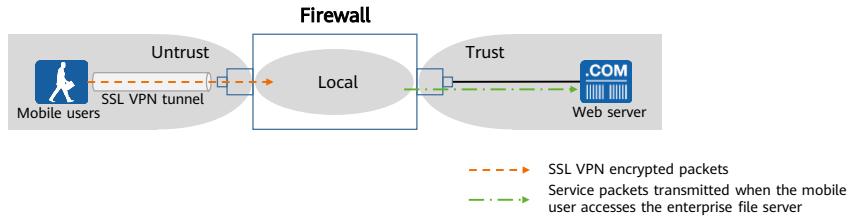
Packet Encapsulation of Web Proxy

- The figure shows the packet encapsulation process when a mobile user accesses intranet web resources. And the access process consists of HTTPS and HTTP sessions.
 - When a mobile user establishes an HTTPS session with the virtual gateway, the source port is 6677, which is a random port and the destination port is 443.
 - When the virtual gateway establishes an HTTP session with the web server, the source port is 9901, which is also a random port, and the destination port is 80.



Key Security Policies in Web Proxy

- When a mobile user accesses the enterprise web server, the packets passing through the firewall are classified into the following types. To ensure the normal use of the web proxy, the following security policies need to be permitted:
 - SSL VPN encrypted packets transmitted between mobile users and the firewall
 - SSL VPN encrypted packets are transmitted from the Untrust zone to Local zone, and permitted by the Untrust-to-Local interzone security policy.
 - Service packets transmitted when the mobile user accesses the enterprise web server
 - Decrypted service packets are transmitted from the Local zone to the Trust zone, and permitted by the Local-to-Trust interzone security policy.



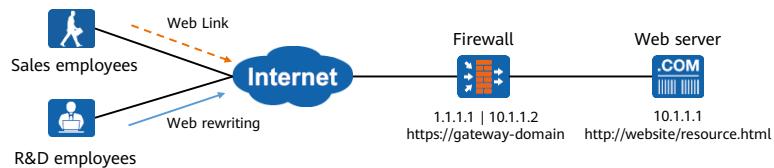
25 Huawei Confidential

HUAWEI

- The security policies for file sharing and port forwarding are the same as those for web proxy. So they are not described anymore.
- Configure a security policy (Internet -> Firewall), which allows mobile users to access the SSL VPN gateway.
 - Source security zone: Untrust; destination security zone: Local;
 - Source IP address: any; source port number: any;
 - Destination IP address: IP address of the SSL VPN gateway; destination port number: port number of the virtual gateway. If the HTTPS port number is changed, enable security policies based on the new port number.
 - Service: HTTPS service;
 - Action: permit.
- Configure a security policy (Firewall -> Intranet), which allows mobile users to access resources at the HQ.
 - Source security zone: Local; destination security zone: Trust;
 - Destination IP address: IP address of the intranet file server;
 - Action: permit.

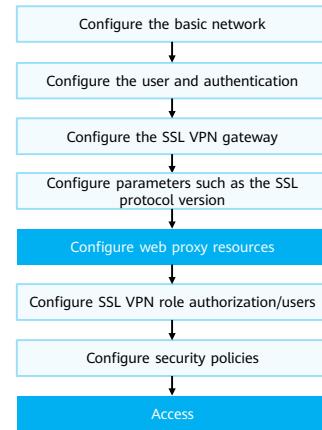
Examples for Configuring the Web Proxy (1/2)

- As shown in the figure, sales and R&D employees of a technology company frequently go on business trips and need to access the enterprise's internal websites. The enterprise deploys a firewall as the security gateway at the network border. The administrator uses the web proxy function of the firewall SSL VPN to provide intranet web applications for mobile users through web link and web rewriting.
- The requirements are as follows:
 - Sales employees need to display official web UIs to customers, and focus on efficiency.
 - R&D employees need to use the developed websites. For security purposes, the specific paths of the developed websites need to be hidden.



Examples for Configuring the Web Proxy (2/2)

- Configuration roadmap:
 - Complete basic network configuration to ensure interconnection.
 - Configure SSL VPN access users and authentication modes.
 - Set SSL VPN gateway parameters, such as the type and gateway address.
 - Set basic SSL parameters, such as the version, algorithm, and cipher suite.
 - Configure web proxy resources, such as the resource name, resource type, and URL.
 - Configure user role authorization.
 - Configure a security policy to permit related traffic.
 - Implement user access.



Configuring Web Proxy Resources

- In **Web Proxy Resource List** area, click **Add** and create a web proxy resource as follows:

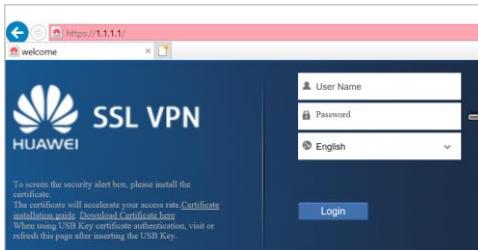
The image shows two side-by-side screenshots of a 'Web Proxy Resource List' dialog box. Both screens have a header 'Add SSL VPN' and a sidebar with navigation links: Gateway Configuration, SSL Configuration, Selected Services, Web Proxy (which is selected), and Role Authorization/User.

Screenshot 1 (Left): The 'Add Resource' dialog is open. The 'Name' field contains 'Web-Server-marketing'. The 'Resource Type' dropdown is set to 'Web Link'. The 'URL' field contains 'http://10.3.0.2:8080'. The 'Description' field is empty. Below the form, a note says 'Note: Enable the security policy to ensure that users can access Web proxy resources. [Add Security Policy]'. At the bottom are 'OK' and 'Cancel' buttons.

Screenshot 2 (Right): The 'Add Resource' dialog is open. The 'Name' field contains 'Web-Server R&D'. The 'Resource Type' dropdown is set to 'Web Rewriting'. The 'URL' field contains 'http://10.3.0.2:8080'. The 'Description' field is empty. Below the form, a note says 'Note: Enable the security policy to ensure that users can access Web proxy resources. [Add Security Policy]'. At the bottom are 'OK' and 'Cancel' buttons.

User Access Verification Configuration (1/2)

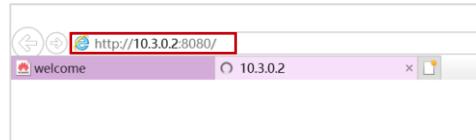
- Enter <https://1.1.1.1:443> in the address bar of the PC browser to access the SSL VPN login page. Install the control as prompted upon the first login.
- On the login page, enter the user name and password and click Login. After the login is successful, the web resource link is displayed on the virtual gateway page.



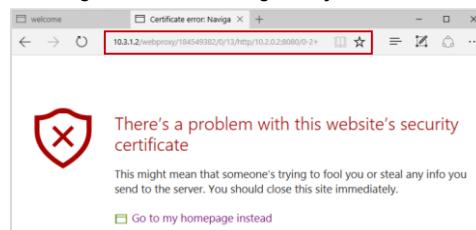
- In the verification phase, resource links in the web proxy are displayed in a centralized manner. A user can view resources of both the marketing and R&D departments.

User Access Verification Configuration (2/2)

- Users can click the web resource link displayed on the virtual gateway page to access the resource.
 - **Web-Server-marketing** is in web link mode. Click to discover the URL, as shown in the following figure.



- **Web-Server-R&D** is in web rewriting mode. The virtual gateway hides the actual URL.

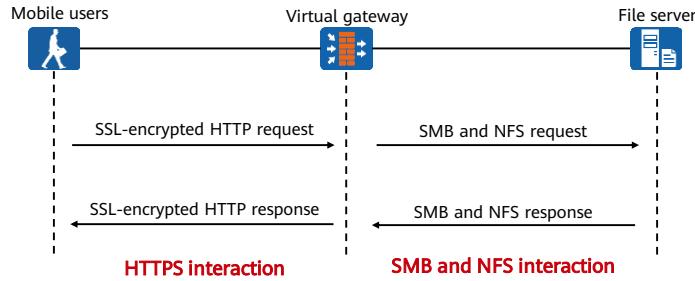


Contents

1. Overview of SSL VPN
2. **Service Functions of SSL VPN**
 - Web Proxy
 - **File Sharing**
 - Port Forwarding
 - Network Extension
3. Examples for Configuring the SSL VPN
4. SSL VPN Troubleshooting

Introduction to File Sharing

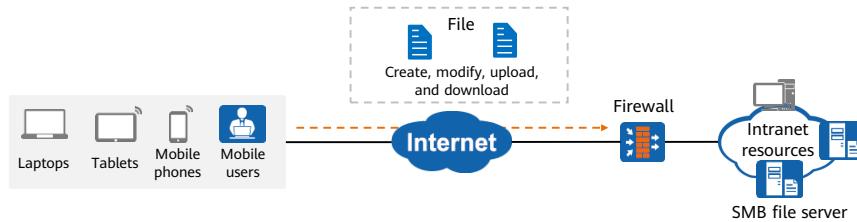
- File sharing is one of the SSL VPN functions. File sharing protocols (SMB and NFS) are converted into SSL-based HTTPS to implement web access to intranet file servers.
- It allows remote access users to securely access internal file servers through browsers and supports common file operations, such as creating, modifying, uploading, and downloading files.



- Currently, file sharing protocols including SMB and NFS are popular in enterprises. SMB is mainly used in Windows, and NFS is mainly used in Linux. Both of them are supported by the SSL VPN of Huawei firewalls.
- As shown in the figure, the firewall can be used as the virtual gateway. The communication between the firewall and the client is encrypted using HTTPS. When the encrypted packets reach the firewall, the firewall decrypts them and performs protocol conversion. Finally, the firewall, as the SMB client, sends requests to the SMB file sharing server. The requests also include the file server authentication process. From the perspective of the protocol used for communication, the preceding process can be divided into two phases:
 - The remote access user functions as the web client to interact with the web server of the firewall through HTTPS.
 - The firewall functions as the SMB client to exchange SMB messages with the SMB server.

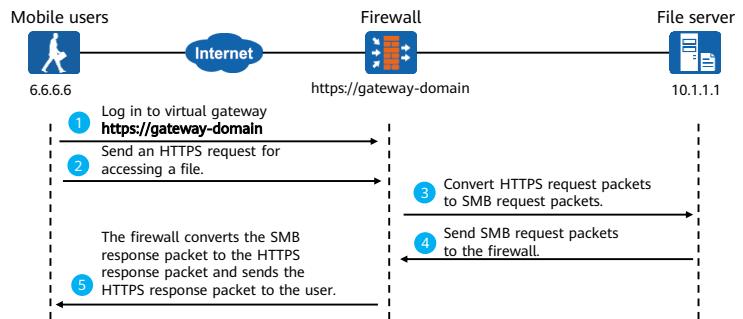
Application Scenario

- In a medium-or large-sized enterprise, multiple SMB file servers are deployed on the intranet, and each file server provides different file resources. Mobile users want to quickly view internal document resources and ensure access security. The file sharing function can meet this requirement.
- As shown in the figure, the file sharing function is used to display the file resources of the SMB server in the form of web links, allowing employees to access intranet file resources. Mobile users can access the intranet file server just like accessing common web UIs. They do not need to install the file sharing client or remember the IP address of the server. They only need to click the link of the file resource on the web UI to access the file server.



Interaction Process of the File Sharing Service

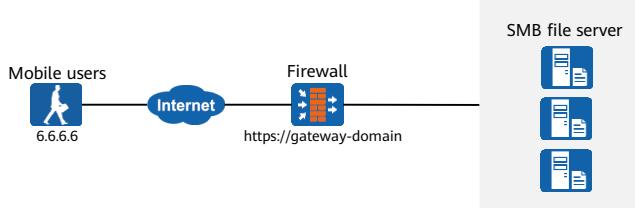
- The file sharing function implements protocol translation when mobile users access intranet file resources. For example, when a mobile user accesses an intranet Windows file server, the process is divided into the following two phases:
 - HTTPS phase: The firewall functions as the web server to receive file access requests from mobile users, and then translates the requests into SMB requests.
 - SMB phase: The firewall functions as the SMB client to initiate requests, receives responses, and then translates the responses to mobile users.



- The figure shows the service interaction process that a mobile user accesses an intranet file server using the file sharing function. The procedure is as follows:
 - The mobile user accesses the virtual gateway through <https://gateway-domain> for SSL VPN login authentication.
 - After logging in to the virtual gateway, the user accessing file sharing resources for the first time must pass the authentication of the file server. This authentication is different from the authentication during SSL VPN login. In the login phase, the user must pass the firewall authentication first. At the same time, to access file sharing resources, you need to check whether the file server has response. When you click **Public_share** in the resource list, the authentication page is displayed. After the file server is successfully authenticated, the mobile user can view the list of accessible file resources on the virtual gateway and click the link of the resource to be accessed.
 - After receiving the HTTPS request, the firewall converts the HTTPS request packet into an SMB packet, and then forwards the SMB packet to the file server.
 - After receiving the SMB request packet, the file server sends SMB response packets to the firewall.
 - After receiving the SMB response packet, the firewall converts the SMB response packet to the HTTPS response packet and returns the HTTPS response packet to the user.

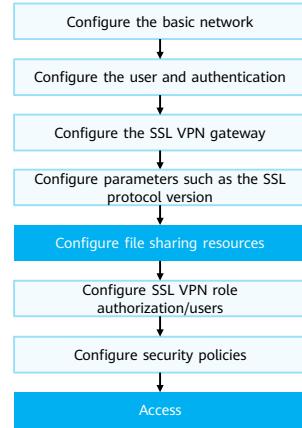
Examples for Configuring the File Sharing (1/2)

- A firewall is deployed at the border of an enterprise network as the security gateway. Multiple SMB file servers are deployed on the intranet, which provide different file resources. The company requires that mobile users can securely and quickly view internal documents on the Internet.
- The requirements are as follows:
 - The administrator uses the file sharing function of the SSL VPN to meet the access requirements of mobile users.
 - Hides the specific path and location of the internal file.



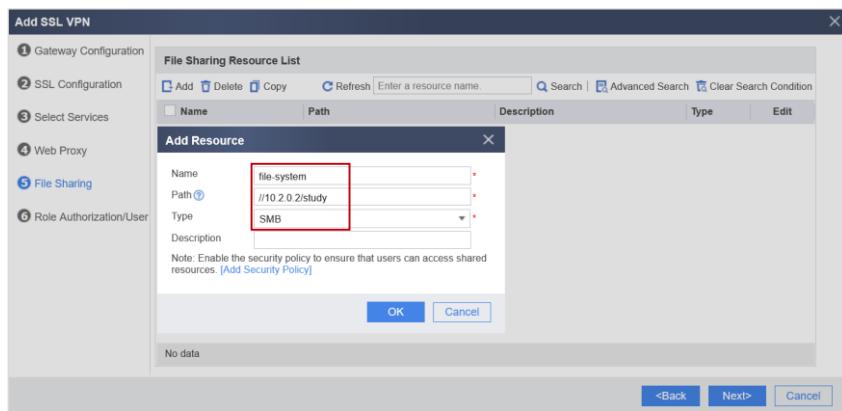
Examples for Configuring the File Sharing (2/2)

- Configuration roadmap:
 - Complete basic network configuration to ensure interconnection.
 - Configure SSL VPN access users and authentication modes.
 - Set SSL VPN gateway parameters, such as the type and gateway address.
 - Set basic SSL parameters, such as the version, algorithm, and cipher suite.
 - Configure file sharing resources, such as the resource name, resource path, and resource type.
 - Configure user role authorization.
 - Configure a security policy to permit related traffic.
 - Implement user access.



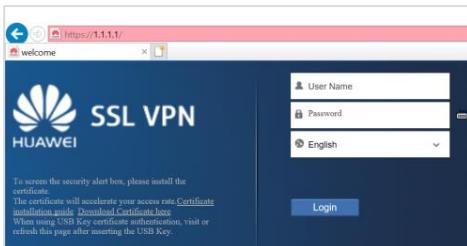
Configure File Sharing Resources

- In **File Sharing Resource List** area, click **Add** and create a file resource as follows:



User Access Verification Configuration Result

- Enter <https://1.1.1.1:443> in the address bar of the browser to access the SSL VPN login page. Install the control as prompted upon the first login.
- On the login page, enter the user name and password and click **Login**. After the login succeeds, the web resource links are displayed on the virtual gateway page. You can click a link to access the resource.

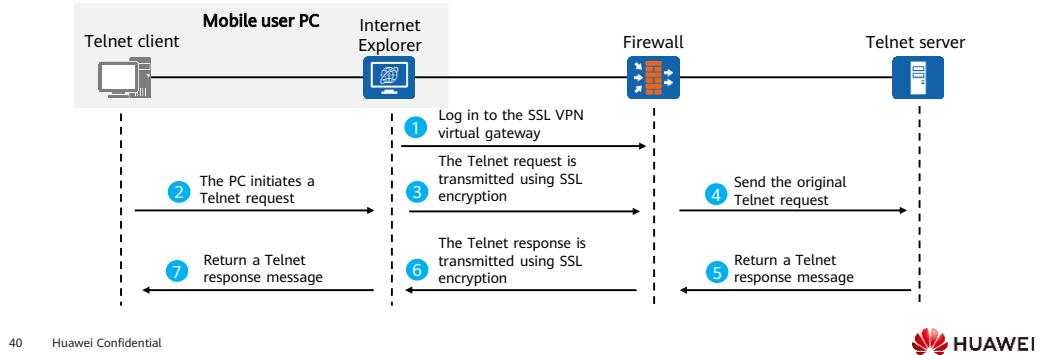


Contents

1. Overview of SSL VPN
2. **Service Functions of SSL VPN**
 - Web Proxy
 - File Sharing
 - Port Forwarding
 - Network Extension
3. Examples for Configuring the SSL VPN
4. SSL VPN Troubleshooting

Overview of Port Forwarding

- In port forwarding mode, TCP packets with specified destination IP addresses and ports are obtained on the client and then forwarded to the intranet through the virtual gateway. In this way, specified TCP resources on the intranet can be accessed.
- TCP resources are TCP-based upper-layer applications, such as Telnet, FTP, and email. The following figure shows the port forwarding process when you log in to the server in Telnet mode.



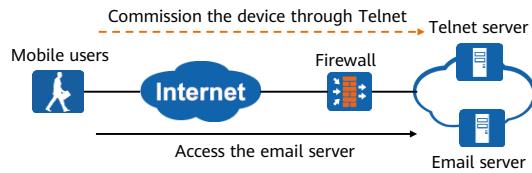
40 Huawei Confidential

HUAWEI

- In the preceding figure, assume that the Telnet IP address is 10.1.1.1. The detailed process is as follows:
 - A user initiates a request using Telnet 10.1.1.1 on the client.
 - The ActiveX plug-in installed on the Internet Explorer identifies the data destined for 10.1.1.1 and the data is forwarded to the virtual gateway of the firewall through vNICs.
 - After receiving the SSL request packet, the firewall virtual gateway decrypts the packet and forwards it to the Telnet server at 10.1.1.1. The firewall establishes a TCP connection with the Telnet server and replies with the Telnet login information.
 - After receiving the Telnet login information, the firewall encapsulates the information into SSL packets and forwards it to the mobile user.
 - After the mobile user receives the packet from the firewall virtual gateway, the ActiveX control decrypts the received SSL-encrypted packet and returns Telnet login information to the client.

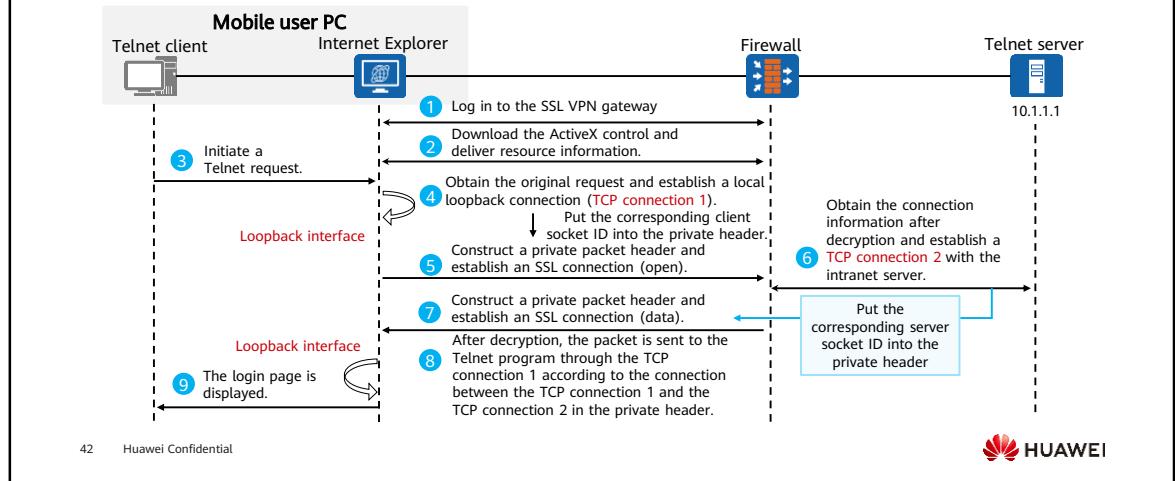
Application Scenario

- In the SSL VPN service functions described earlier, web proxy and file sharing are common fine-grained resources. However, the enterprise still needs to access TCP-based non-web applications. In this case, the enterprise can use the port forwarding function of SSL VPN to forward Internet requests to the intranet, which can meet users' requirements for accessing TCP-based resources.
- As shown in the figure, mobile users want to remotely commission various network devices on the enterprise network through Telnet and access the email server. To meet these requirements, you can use the port forwarding function of SSL VPN to encrypt packets and ensure the confidentiality of packet interaction.



Interaction Process of Port Forwarding Service

- The following describes the working process of the port forwarding service when a mobile user uses a Telnet client to access an intranet Telnet server.

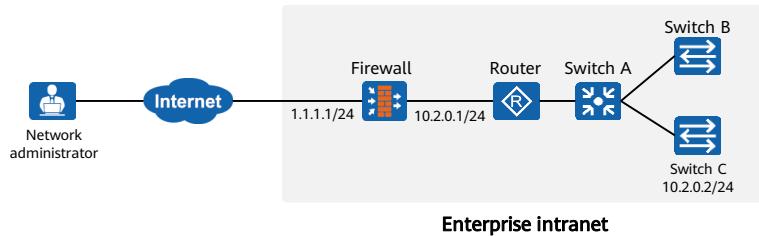


- The key technology of port forwarding is forwarding client at the port. After a user logs in to the virtual gateway using the Internet Explorer of the Windows OS, the port forwarding client (ActiveX control) automatically runs on the Internet Explorer of the local PC. The client is used to listen to all requests of other programs in real time, intercepts the requests sent by mobile users to the intranet server, and then sends these requests to the virtual gateway through the SSL connection. These requests are intercepted based on the configuration of the virtual gateway. The configured port forwarding resources are the instructions delivered by the virtual gateway to the port forwarding client. When a user accesses intranet TCP resources, the port forwarding client assists the user in completing the access. In the port forwarding function, the delivered command includes the IP address of the destination host and the destination port. The preceding information determines the application resources to be accessed by the mobile user.

- The figure shows the service interaction process when a mobile user accesses the Telnet server on the intranet in port forwarding mode. The procedure is as follows:
 - Open the browser, enter <https://SSL VPN server address: port number or https://domain name> in the address box to initiate a connection.
 - After you log in to the virtual gateway through the Internet Explorer of the Windows OS, the port forwarding client (ActiveX control) automatically runs and listens to the request according to the resource information delivered by the virtual gateway.
 - The port forwarding client listens to the request from the computer at any time. If the resource information (destination IP address and destination port) delivered by the virtual gateway matches request, the client immediately intercepts the TCP SYN packet and uses the local loopback interface (127.0.0.1), as the receiver, to simulate the receiving of a Telnet service request (TCP connection).
 - Adds the socket ID of TCP connection 1 to the constructed private packet header, and sends the packet to the virtual gateway after SSL encryption.
 - After receiving the SSL-encrypted packet, the virtual gateway decrypts it and obtains the real destination IP address, port number, and command word from the private packet header. Then the virtual gateway functions as the Telnet client to establish a Telnet connection with the intranet server.
 - After receiving the response packet (login page) from the intranet server, the virtual gateway constructs a private packet header and fills in the socket ID of TCP connection 2 (server socket ID) before sending the packet to the remote client. In this way, the mapping between TCP connection 2 and TCP connection 1 is established.
 - The virtual gateway sends the SSL-encrypted private packet header and data to the port forwarding client. The port forwarding client finds TCP connection 1 based on the client socket ID in the private packet header, finds the real IP address of the Telnet client based on the local loopback record table, and returns the real data.

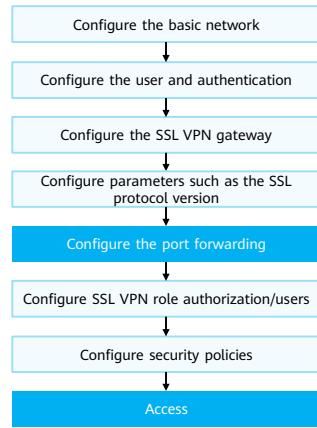
Examples for Port Forwarding (1/2)

- Firewalls are deployed at the enterprise network border as the security gateway. The enterprise has many routers, switches, and servers. The network administrator is on a business trip and needs to use the port forwarding function of SSL VPN to remotely log in to the network device (10.2.0.2/24) on the enterprise intranet through Telnet for management.



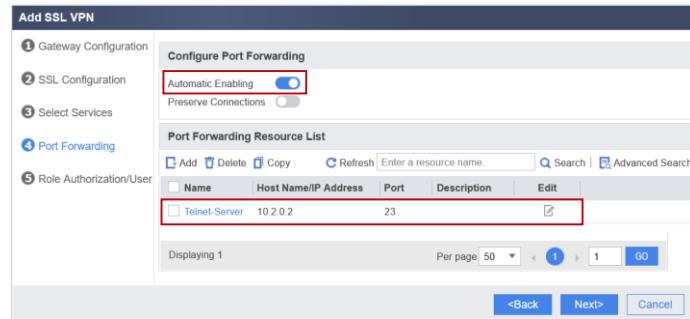
Examples for Port Forwarding (2/2)

- Configuration roadmap:
 - Complete basic network configuration to ensure interconnection.
 - Configure SSL VPN access users and authentication modes.
 - Set SSL VPN gateway parameters, such as the type and gateway address.
 - Set basic SSL parameters, such as the version, algorithm, and cipher suite.
 - Configure the port forwarding function, such as the resource name, host address type, and port.
 - Configure user role authorization.
 - Configure a security policy to permit related traffic.
 - Implement user access.



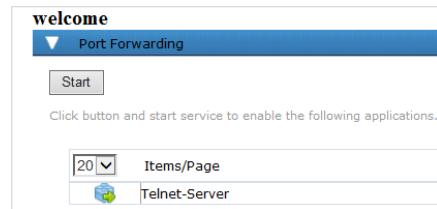
Configuring the Port Forwarding

- In the **Port Forwarding** tab page, enable **Automatic Enabling**. In the **Port Forwarding Resource List** area, click **Add** and configure port forwarding resources as follows:



User Access Verification Configuration Result

- Enter <https://1.1.1.1:443> in the address bar of the PC browser to access the SSL VPN login page. Install the control as prompted upon the first login.
- On the login page, enter the user name and password and click **Login**. After the login is successful, the port forwarding resource is displayed on the virtual gateway page. You can click the link to access the resource.



Contents

1. Overview of SSL VPN
2. **Service Functions of SSL VPN**
 - Web Proxy
 - File Sharing
 - Port Forwarding
 - Network Extension
3. Examples for Configuring the SSL VPN
4. SSL VPN Troubleshooting

Introduction to Network Extension

- Although the web proxy, file sharing, and port forwarding functions allow mobile users to access internal resources, these functions support only specific protocols. If a user needs to access the internal voice server for a conference call, the preceding functions cannot meet this requirement because the voice service is generally implemented based on UDP.
- The SSL VPN network extension function supports the establishment of network-layer VPN tunnels, helping users access richer resources and enabling mobile users to access enterprise IP services.

HTTP or HTTPS (web proxy), Telnet, SSH,
SMB or NFS (file sharing), FTP, SMTP, etc

Application layer protocol

TCP (port forwarding) and UDP

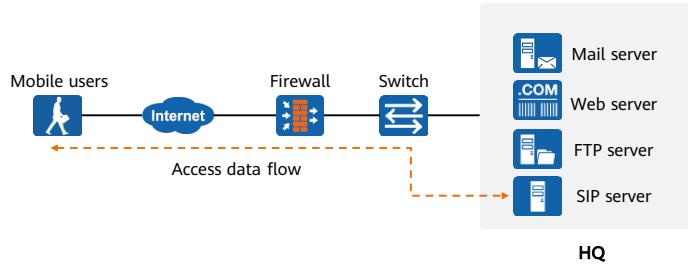
Transport layer protocol

IP (network extension) and IPv6

Network layer protocol

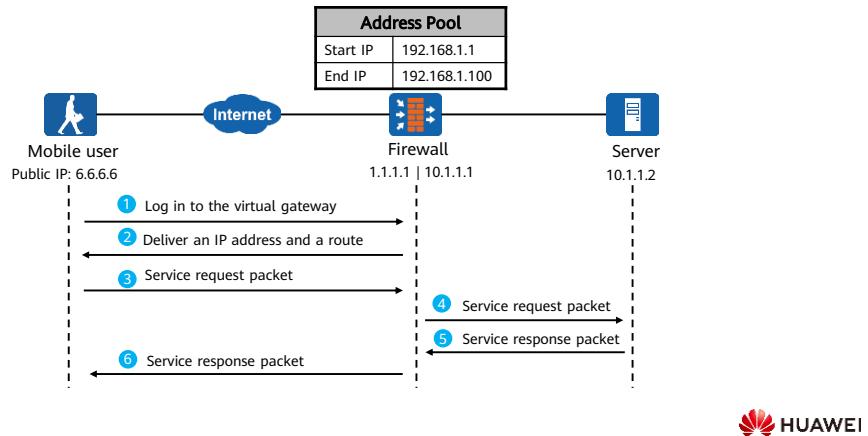
Application Scenario

- Large- and medium-sized enterprises have multiple complex functions, such as video conferencing and financial systems. To use these functions, the SSL VPN network extension function is used to implement mobile user access.
- As shown in the figure, the HQ provides the SIP voice service. So, a certain technology needs to be used to protect the communication between the mobile user and the intranet SIP server. In addition, the mobile user needs to access intranet resources as if they were on the LAN. In this case, the SSL VPN network extension function can be used to allow mobile users to access resources at the HQ.



Interaction Process of Network Extension Service

- A mobile user establishes an SSL VPN with the virtual gateway and uses the network extension function to access intranet resources. The internal interaction process is as follows:

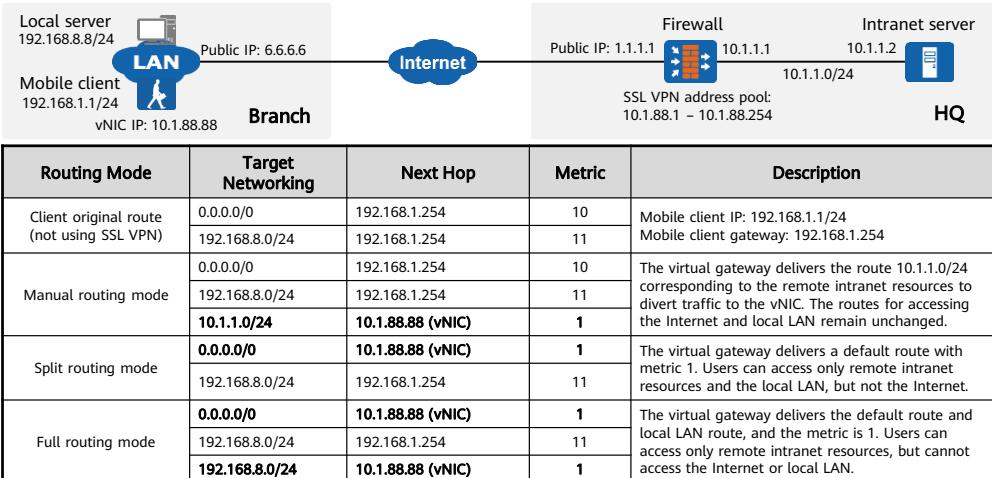


51 Huawei Confidential

HUAWEI

- The figure shows the service interaction process that a mobile user accesses server resources through the network extension function. The procedure is as follows:
 - The mobile user logs in to the virtual gateway through the web browser.
 - After login, the user enables the network extension function. After the network extension function is enabled:
 - The user establishes an SSL VPN tunnel with the virtual gateway;
 - The user's local PC automatically generates a vNIC. The virtual gateway assigns an IP address in the address pool to the vNIC for communication between the user and intranet server. With the IP address, the mobile user can access intranet IP resources as an intranet user does.
 - The virtual gateway delivers the route to the intranet server to the user. The virtual gateway delivers routes to the user based on the network extension configuration.
 - The user sends a service request packet to the intranet server. The packet reaches the virtual gateway over an SSL VPN tunnel.
 - The virtual gateway receives the request packet, decapsulates it, and then forwards it to the intranet server.
 - The intranet server returns a service response packet to the user.
 - The virtual gateway receives the response packet and forwards it to the user over the SSL VPN tunnel. The user receives the response packet and decapsulates it to obtain the required information.

Routing Mode



52 Huawei Confidential

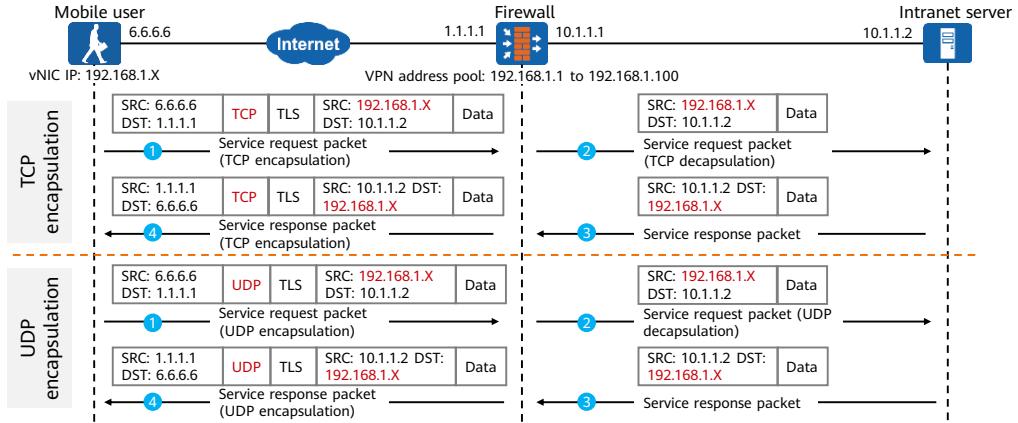


- The topology shows that:

- The mobile client is located in the branch and obtains the branch intranet IP address 192.168.1.1/24. The gateway address is 192.168.1.254.
 - The local server address of the branch is 192.168.8.8/24. The mobile client has a route 192.168.8.0/24 with the next hop pointing to the gateway address 192.168.1.254.
 - The mobile client connects to the HQ through SSL VPN. After the connection is successful, the IP address obtained by the vNIC is 10.1.88.88. The address pool of the SSL VPN virtual gateway ranges from 10.1.88.1 to 10.1.88.254.
 - The IP address range of the intranet resource provided by the HQ is 10.1.1.0/24.

Packet Encapsulation

- There are two packet encapsulation modes for the network extension function: reliable transmission mode (TCP encapsulation) and quick transmission mode (UDP encapsulation).



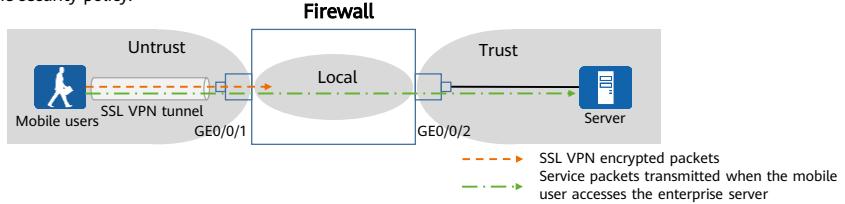
53 Huawei Confidential

HUAWEI

- The reliable transmission mode is recommended when the network environment is unstable. If the network environment is stable, you are advised to use the fast transmission mode to improve data transmission efficiency.

Key Security Policies in Network Extension

- When a mobile user accesses an enterprise server, the packets passing through the firewall are classified into the following types. And the security policy processes these types of packets accordingly.
 - SSL VPN encrypted packets transmitted between mobile users and the firewall
 - SSL VPN encrypted packets are transmitted from the Untrust zone to Local zone and permitted by the Untrust-to-Local interzone security policy.
 - Service packets transmitted when the mobile user accesses the enterprise server
 - Decrypted service packets are transmitted from the Untrust zone to the Trust zone, and the traffic is permitted by the Untrust-to-Trust interzone security policy.



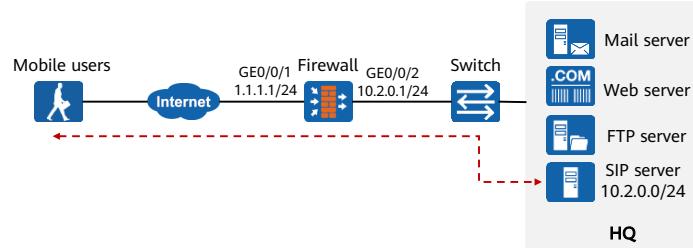
54 Huawei Confidential

 HUAWEI

- When a mobile user accesses the enterprise server, the destination security zone that the decrypted service packets passes through is the Trust zone, and the source security zone is the security zone where the inbound interface of the service packets resides. The inbound interface of service packets is GE0/0/1. As GE0/0/1 resides in the Untrust zone, the source security zone of decrypted packets is the Untrust zone.
- Configure a security policy (Internet -> Firewall), which allows mobile users to access the SSL VPN gateway.
 - Source security zone: Untrust; destination security zone: Local;
 - Source IP address: any; source port number: any;
 - Destination IP address: IP address of the SSL VPN gateway; destination port number: port number of the virtual gateway. If the HTTPS port number is changed, enable security policies based on the new port number.
 - Service: HTTPS service;
 - Action: permit.
- Configure a security policy (Mobile users -> Intranet), which allows mobile users to access resources at the HQ.
 - Source security zone: Untrust; destination security zone: Trust;
 - Source address: IP address range obtained by mobile users; source port number: any;
 - Destination IP address: IP address of the intranet file server; destination port number: port number of the intranet web server;
 - Action: permit.

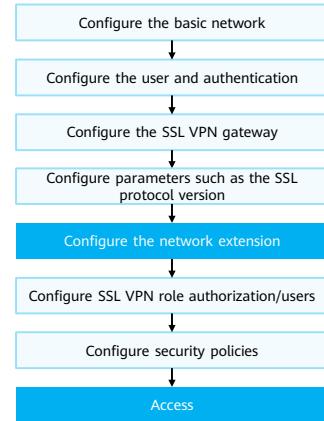
Examples for Configuring the Network Extension (1/2)

- Firewalls are deployed at the enterprise network border as the security gateway. Mobile users need to access various server resources on the intranet. When the voice conference is needed, they need to connect to the SIP server at the HQ whose IP address is on the network segment 10.2.0.0/24. The administrator uses the network extension function of SSL VPN to meet this requirement.



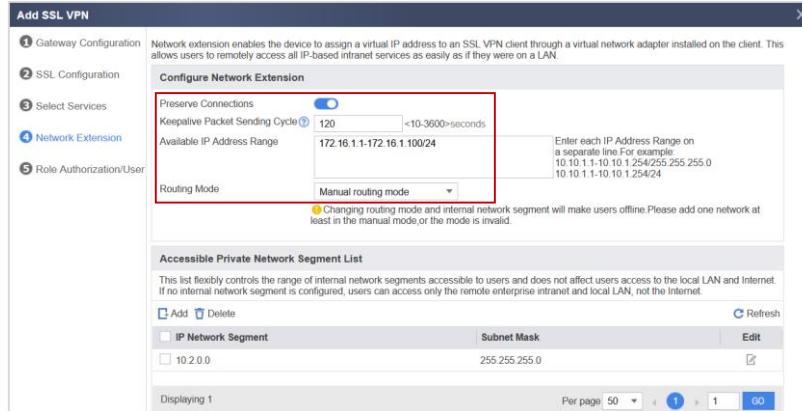
Examples for Configuring the Network Extension (2/2)

- Configuration roadmap:
 - Complete basic network configuration to ensure interconnection.
 - Configure SSL VPN access users and authentication modes.
 - Set SSL VPN gateway parameters, such as the type and gateway address.
 - Set basic SSL parameters, such as the version, algorithm, and cipher suite.
 - Configure the network extension function, including keepalive, allocatable IP address range, and routing mode.
 - Configure user role authorization.
 - Configure a security policy to permit related traffic.
 - Implement user access.



Configuring the Network Extension

- Choose **Network > SSL VPN > SSL VPN**, click **Add**, and configure network extension resources as follows:



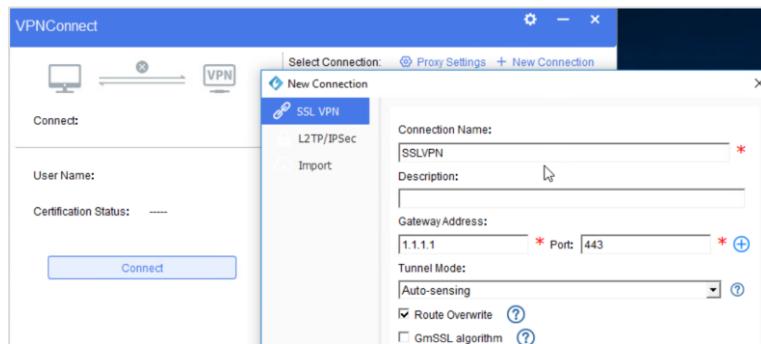
User Access Verification Configuration (1/3)

- Enter **https://1.1.1.1:443** in the address bar of the PC browser to access the SSL VPN login page. Install the control as prompted upon the first login.
- On the login page, enter the user name and password and click **Login**. After the login is successful, click **User Options** to download and install the network extension client.



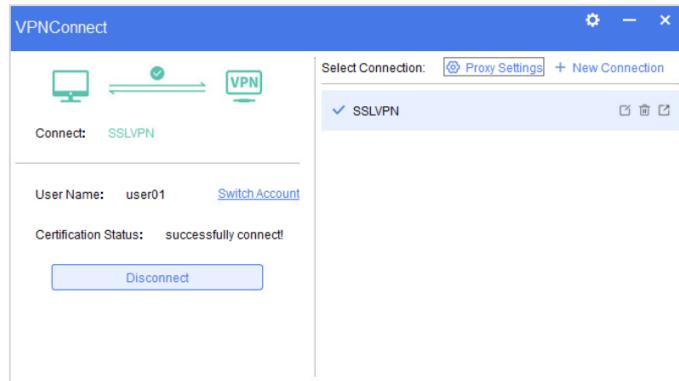
User Access Verification Configuration (2/3)

- Use the installed client software to log in to the SSL VPN.



User Access Verification Configuration (3/3)

- After successful login, you can access intranet resources.

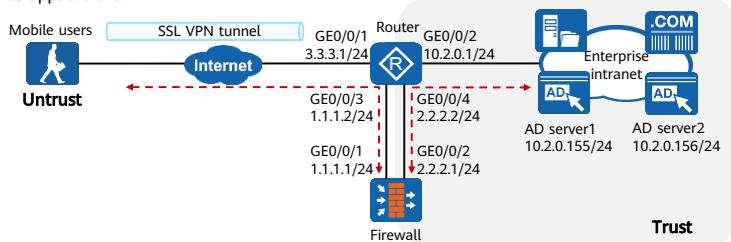


Contents

1. Overview of SSL VPN
2. Service Functions of SSL VPN
- 3. Examples for Configuring the SSL VPN**
4. SSL VPN Troubleshooting

Examples for Configuring the SSL VPN (1/4)

- The preceding figure shows the networking of an enterprise. The details are as follows:
 - Router: Functions as the gateway and egress device of the enterprise intranet server. GE0/0/1 connects to the Internet; forwards the requests for establishing SSL VPN between mobile users through the NAT server and the firewall; and forwards the data that mobile users access intranet services.
 - Firewall: The firewall is deployed in off-path mode on the router side as the SSL VPN virtual gateway to forward the access of mobile users to the intranet.
 - Server: The AD server authenticates the identity of mobile users and authorizes mobile users to access resources. Other servers provide service applications.



Examples for Configuring the SSL VPN (2/4)

- The enterprise requires that mobile users can access resources at the HQ through SSL VPN and that access users be authenticated. The requirements are as follows:
 - Common employees can remotely access the Webmail and ERP systems on web UIs.
 - Senior executives can use clients to dial up to the SSL VPN and obtain private IP addresses when they are on business trips or working at home. In this way, they can use various intranet resources as if they were working on the intranet. They also need to remotely access the Webmail and ERP systems on web UIs.
 - An AD server has been deployed on the live network. Access users need to access intranet resources after identity authentication.
 - Security check is performed on endpoints that access the enterprise intranet. If no antivirus software is installed, the access is prohibited.
- The network extension and web proxy of the SSL VPN technology are used to meet the preceding requirements.
 - Network extension: Senior executives can access intranet resources when they are on business trips or working at home.
 - Web proxy: Both senior executives and common employees can access the enterprise Webmail and ERP systems through web UIs.

Examples for Configuring the SSL VPN (3/4)

- The following table lists the interface IP addresses of devices on the network and SSL VPN parameters.

Item	Data
Router interface	Interface number: GigabitEthernet 0/0/1 IP address: 3.3.3.1/24
	Interface: GigabitEthernet 0/0/2 IP address: 10.2.0.1/24
	Interface number: GigabitEthernet 0/0/3 IP address: 1.1.1.2/24
	Interface number: GigabitEthernet 0/0/4 IP address: 2.2.2.2/24
Firewall interface	Interface number: GigabitEthernet 0/0/1 IP address: 1.1.1.1/16 Security zone: Untrust
	Interface: GigabitEthernet 0/0/2 IP address: 2.2.2.1/16 Security zone: Trust
AD server1 address	IP address: 10.2.0.155/24 Gateway: 10.2.0.1/24
AD server2 address	IP address: 10.2.0.156/24 Gateway: 10.2.0.1/24

Table 1 IP address plan

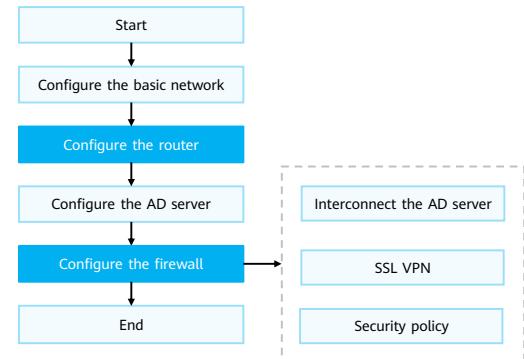
Item	Data
Mobile user account	Senior executives User name: user_0001 Group: /cce.com/director
	Common employee User name: user_0002 Group: /cce.com/employee
Firewall virtual gateway	Name: example Interface: GigabitEthernet 1/0/1 Domain name: example.huawei.com Maximum number of users: 150 Maximum number of concurrent users: 100
AD server	Primary server IP address: 10.2.0.155 Secondary server IP address: 10.2.0.156
Web proxy resource	Name: Webmail; link: http://10.2.0.10 Name: ERP; link: http://10.2.0.11
Network extension	Network extension address pool: 172.16.1.1–172.16.1.100 Routing mode: manual Internal network segment accessible to network extension users: 10.2.0.0/16

Table 2 SSL VPN data plan



Examples for Configuring the SSL VPN (4/4)

- Configuration roadmap:
 - Complete basic network configurations, including setting IP addresses for firewall interfaces and adding firewall interfaces to security zones.
 - Configure the router, including the NAT server, PBR, and default route.
 - Complete the basic configuration of the AD server.
 - Configure the firewall, including AD server interconnection parameters, SSL VPN configurations, and necessary security policies.



- For details about how to configure basic IP addresses for interfaces on each device, see the previous slide.
- Step 3: Configure the AD server. This section does not describe how to configure the AD server.

Configuring the Router

- Configure the router
 - Configure the NAT server, and then forward SSL VPN establishment requests of mobile users and intranet access data to the firewall.

```
[Router] interface GigabitEthernet 0/0/1
[Router-GigabitEthernet0/0/1] nat server protocol tcp global 3.3.3.1 443 inside 1.1.1.1 443
```
 - Configure the PBR, and then forward the data returned by the server to mobile users to the firewall.

```
[Router] acl number 3000
[Router-acl-adv-3000] rule permit ip source 10.2.0.0 0.0.0.255

[Router] traffic classifier internal
[Router-classifier-internal] if-match acl 3000
[Router] traffic behavior internal
[Router-behavior-internal] redirect ip-nexthop 2.2.2.1
[Router] traffic policy internal
[Router-trafficpolicy-internal] classifier internal behavior internal

[Router] interface GigabitEthernet 0/0/2
[Router-GigabitEthernet0/0/2] traffic-policy internal inbound
```
 - Configure a default route to the Internet, and then forward the reply data encrypted by the firewall to the mobile user.

```
[Router] ip route-static 0.0.0.0 0 3.3.3.2
```

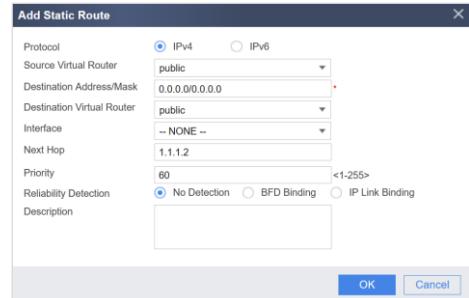
Configuring the Firewall - Security Zone

- Firewall configurations include route interworking, SSL VPN web proxy, network extension, and security policies.
 - Choose **Network > Interface**, edit GE0/0/1, and add GE0/0/1 to the Untrust zone. Add GE0/0/2 to the Trust zone in the same way.

The screenshot shows a configuration interface for a GigabitEthernet interface. The 'Interface Name' is set to 'GigabitEthernet0/0/1'. The 'Virtual System' dropdown is set to 'public'. The 'Zone' dropdown is set to 'untrust'. Under the 'Mode' section, the 'Routing' radio button is selected, while 'Switching', 'Bypass', and 'Interface Pair' options are unselected. The entire interface is enclosed in a dark blue header bar labeled 'Modify GigabitEthernet Interface'.

Configuring the Firewall - Default Route

- Choose **Network > Route > Static Route** and create a route from the firewall to the intranet.
- Choose **Network > Route > Static Route** and create a route from the firewall to the external network.



Configuring the Firewall-AD Interconnection Parameters

- Choose **Object > Authentication Server > AD** and set parameters for communication between the firewall and AD server.

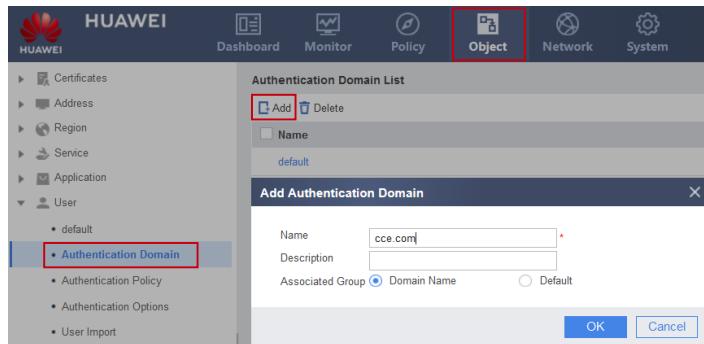
The screenshot shows the HUAWEI Firewall management interface. On the left, there is a navigation tree with various icons and sections like Certificates, Address, Region, Service, Application, User, Device, and Authentication Server (which is expanded to show RADIUS, HWTCACCS, and AD). The 'Object' tab is selected. In the main area, there's a 'Dashboard' with several cards, a 'Monitor' section, and a 'Policy' section. Below these is the 'Object' section, which is currently active. Under 'Object', there's a 'Network' section with a 'Firewall' card. The 'Authentication Server' section is also visible, with 'AD' selected. A red box highlights the 'AD' button in the navigation tree and the 'Add' button in the 'AD Server List' table. To the right, a detailed configuration dialog box titled 'Modify AD Server' is open. It contains fields for Primary Authentication Server IP Address (10.2.0.156), Primary Authentication Server Host Name (info-server1.cce.com), Secondary Authentication Server IP Address (10.2.0.156), Secondary Authentication Server Host Name (info-server2.cce.com), Third Authentication Server IP Address (10.2.0.156), and Third Authentication Server Host Name (info-server3.cce.com). There are tabs for 'Source Address Configuration' (set to 'IP Address') and 'Source IP Address'. The 'Basic Information' section includes fields for Base DN/Port DN (dc=cce,dc=cce), LDAP Port (389), sAMAccountName (ou), Bind Anonymous Administrator (unchecked), Administrator DN (cn=Administrator,cn=users), Administrator Password (*****), Confirm Administrator Password (*****), Administrator Binding Attribute (checkbox checked), and Cipher Suite (aes256-tnarc-sha1). At the bottom of the dialog are 'Test', 'OK', and 'Cancel' buttons. A note at the top of the dialog says: 'The third-party authentication server may lack security mechanisms such as password complexity verification and brute force cracking prevention.'

69 Huawei Confidential

HUAWEI

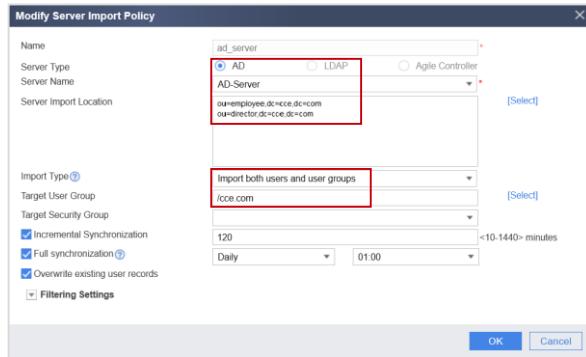
Configuring an Authentication Domain

- Create an authentication domain. The configured authentication domain name must be the same as the domain name on the authentication server.
 - Choose **Object > User > Authentication Domain** and click **Add** to create an authentication domain.



Importing Policy (1/2)

- Configure a server import policy on the firewall to prepare for importing users and organizational structures on the server.
 - Choose **Object > User > User Import > Server Import**, and click **Add** to create a server import policy.

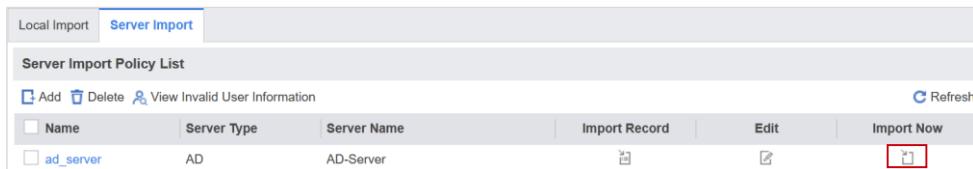


71 Huawei Confidential

 HUAWEI

Importing Policy (2/2)

- Import users and organizational structures on the AD authentication server for subsequent group application.
 - After the policy is created, click  to import the organizational structures from the authentication server to the firewall.



- Then, choose **Object > User > default > User/User Group/Security Group Management List**, you can view the imported user and organizational structure information.

Configuring the SSL VPN Access Mode

- Configure SSL VPN access user management and specify an authentication server to the user.
 - Choose **Object > User** and select cce.com. Select **SSL VPN Access** and specify the AD server.

The screenshot shows the 'User Management' interface. In the 'Scenario' section, the 'SSL VPN access' checkbox is selected. In the 'User Configuration' section, 'Authentication Server' is checked and set to 'AD\AD-Server'. Below this is a table titled 'User/User Group/Security Group Management List' showing two users: 'employee@cce.com' and 'director@cce.com'. Both users are associated with the '/cce.com' user group and have 'local' as their source. The 'Expiration Time' column shows 'Never' for both. The 'Edit' column contains checkboxes for each user. At the bottom right of the interface is a blue 'Apply' button.

Name	Description	User Group	Source	Binding Infor...	Expiration Time	Activat...	Edit
employee@cce.com		/cce.com	local	None	Never	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
director@cce.com		/cce.com	local	None	Never	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

73 Huawei Confidential



Configuring the Authorization Mode

- Configure the authorization mode to AD server authorization.
 - Configure the authorization mode to AD server authorization. You need to log in to the CLI console to configure the authorization mode because it cannot be configured on the web UI. Click the **CLI Console** dialog box in the lower right corner of the page to connect to the CLI console. After the connection is successful, configure the following commands:

```
<FW> system-view
[FW] aaa
```
 - Create authorization scheme **ad** and configure **authorization-mode ad**.

```
[FW-aaa] authorization-scheme ad
[FW-aaa-author-ad] authorization-mode ad
[FW-aaa-author-ad] quit
```
 - Apply the authorization scheme to the authentication domain.

```
[FW-aaa] domain cce.com
[FW-aaa-domain-cce.com] authorization-scheme ad
```

Configuring the SSL VPN (1/7)

- Configure an SSL VPN gateway, including the gateway address, user authentication, and maximum number of concurrent users.
 - Choose Network > SSL VPN > SSL VPN, click Add, and set the parameters as follows:

The screenshot shows the Huawei Network Management System interface. On the left, there is a navigation tree with various network components like Interface, VLAN, DNS, DHCP Server, Route, IPsec, L2TP, GRE, DSVPN, and SSL VPN. Under SSL VPN, the 'SSL VPN' item is selected and highlighted with a red box. In the center, there is a 'SSL VPN List' table with columns: Gateway Name, Gateway IP Address:Port, and Domain Name. A red box highlights the 'Add' button. To the right, a detailed configuration dialog titled 'Add SSL VPN' is open. It has several tabs: 1. Gateway Configuration: Set Gateway Name to 'example', Type to 'Exclusive', and Gateway IP Address to '192.168.1.1'. Port is set to 443. Note: 'Enable the security policy to ensure that users log in to the gateway.' 2. SSL Configuration: Set Client CA Certificate to 'default' and Certificate Authentication to 'NONE'. 3. Select Services: Set Authentication Domain to 'cce.com'. 4. Role Authorization/User: Set Primary DNS Server to '443', Secondary DNS Server 1 to '10', Maximum Concurrent Users to '500', and Maximum Resources to '1024'. At the bottom right of the dialog are 'Back', 'Next', and 'Cancel' buttons.

Configuring the SSL VPN (2/7)

- Retain the default settings of SSL parameters and click **Next**.

Add SSL VPN

SSL Version TLS 1.0 TLS 1.1 TLS 1.2

If SM2 is selected, the VPN client must support the SM2 algorithm. VPN clients that use RSA cannot log in. Changing the public key algorithm will log out all users of the corresponding gateway.

Public Key Algorithm RSA SM2
Local Certificate

Encryption Suite 256-bit AES Encryption with RSA and a SHA MAC
 128-bit AES Encryption with RSA and a SHA MAC

Session Timeout <1-1440>minutes The default value is 5.

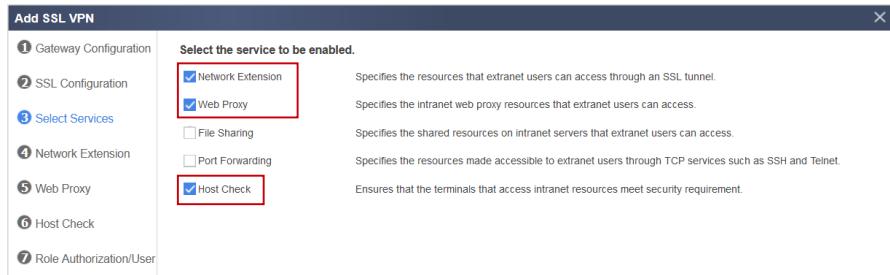
Unrestricted Life Cycle

Life Cycle <60-2880>minutes The default value is 1440.

<Back **Next>** Cancel

Configuring the SSL VPN (3/7)

- Set SSL service parameters.
 - Select the services to be enabled: **Web Proxy**, **Network Extension**, and **Host Check**.



Configuring the SSL VPN (4/7)

- To configure network extension, set parameters such as the range of the allocatable IP address pool and accessible intranet network segment as follows:
- To configure the web proxy, in the **Web Proxy Resource List** area, add resources Webmail and ERP, and click **Add**.

The left screenshot shows the 'Configure Network Extension' section of the 'Add SSL VPN' configuration. It includes fields for 'Keepalive Packet Sending Cycle' (set to 100), 'Available IP Address Range' (set to 192.16.1.5-172.16.1.100/24), and 'Routing Mode' (set to 'Manual routing mode'). The right screenshot shows the 'Web Proxy Resource List' page, which is currently empty. A red box highlights the 'Add' button.

Configuring the SSL VPN (5/7)

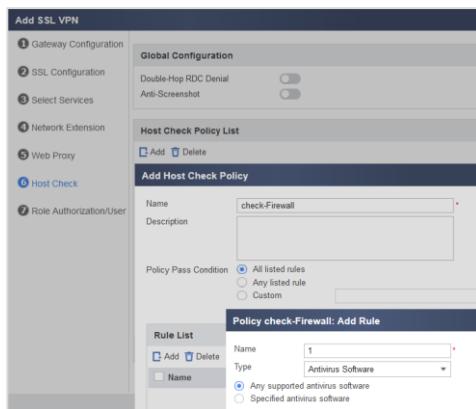
- To configure the web proxy, add web proxy resources Webmail and ERP as follows:

The image displays two separate 'Add Resource' dialog boxes side-by-side. Both dialogs have a similar layout with fields for Name, Resource Type, URL Display Status, URL, Resource Group, and Description. The first dialog is for 'Webmail' and the second is for 'ERP'. Both dialogs show 'Web Rewriting' selected in the Resource Type dropdown and 'Display' checked in the URL Display Status checkbox. The URLs are set to 'http://10.2.0.10' for Webmail and 'http://10.2.0.11' for ERP. The resource groups are both set to '- NONE -'. The descriptions are empty. A note at the bottom of each dialog states: 'Note: Enable the security policy to ensure that users can access Web proxy resources. [Add Security Policy]'. Each dialog has 'OK' and 'Cancel' buttons at the bottom.

Resource	Name	Resource Type	URL Display Status	URL	Resource Group	Description
Webmail	Webmail	Web Rewriting	Display	http://10.2.0.10	- NONE -	
ERP	ERP	Web Rewriting	Display	http://10.2.0.11	- NONE -	

Configuring the SSL VPN (6/7)

- To configure host check, add host check rules based on the following parameters. Then install any device supported antivirus software on the host.

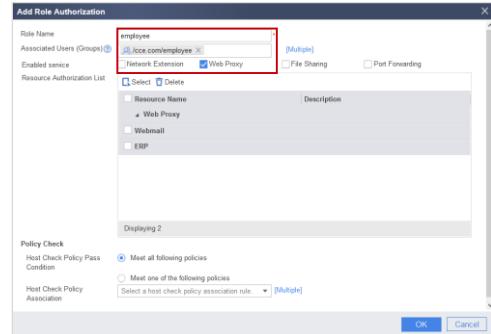
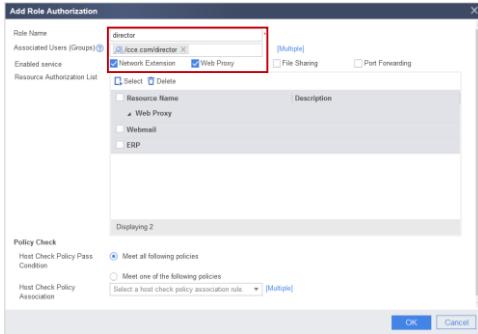


80 Huawei Confidential

 HUAWEI

Configuring the SSL VPN (7/7)

- Configure SSL VPN role authorization/user: Add a role to the **director** group and select corresponding permissions.
- Configure SSL VPN role authorization/user: Add a role to the **employee** group and select corresponding permissions.



Configuring Security Policies (1/2)

- Configure security policies to allow mobile users to log in to the virtual gateway and allow mobile users in network extension mode to access intranet resources. Configure security policies as follows:
 - Permit the traffic transmitted between the Untrust zone and the Local zone to allow mobile users to log in to the virtual gateway.
 - Permit the traffic transmitted between the Untrust zone and the Trust zone to allow mobile users to access the enterprise intranet.

The image contains two side-by-side screenshots of a network configuration interface, likely from a Huawei device. Both screenshots show the 'General Settings' and 'Source and Destination' sections of a policy configuration screen.

Left Screenshot (Policy 1):

- General Settings:** Name: untrust->local, Description: (empty), Policy Group: - NONE -, Tag: (empty).
- Source and Destination:** Source Zone: untrust, Destination Zone: local, Source Address/Region: 1.1.1.1/24, Destination Address/Region: 10.2.0.0/24.

Right Screenshot (Policy 2):

- General Settings:** Name: untrust->trust, Description: (empty), Policy Group: - NONE -, Tag: (empty).
- Source and Destination:** Source Zone: untrust, Destination Zone: trust, Source Address/Region: (empty), Destination Address/Region: 10.2.0.0/24.

Configuring Security Policies (2/2)

- Configure security policies to allow mobile users in web proxy mode to access intranet resources.

Configure security policies as follows:

- Permit the traffic transmitted between the Local zone and the Trust zone to allow mobile users to access the enterprise intranet through web proxy.

The screenshot shows a configuration interface for a security policy. On the left, there's a sidebar with tabs: 'General Settings' (selected), 'Source and Destination' (selected), and 'Advanced'. The 'General Settings' tab has fields for 'Name' (local->trust), 'Description' (empty), 'Policy Group' (-- NONE --), and 'Tag' (Select or enter a tag). The 'Source and Destination' tab has sections for 'Source Zone' (local selected, trust available), 'Destination Zone' (trust selected, local available), 'Source Address/Region' (empty), and 'Destination Address/Region' (10.2.0.0/24 entered).

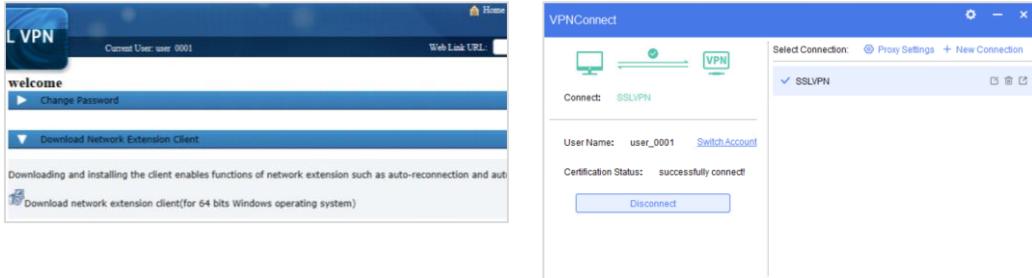
User Access Verification Configuration (1/3)

- Enter <https://3.3.3.1:443> in the address bar of the PC browser to access the SSL VPN login page. Install the control as prompted upon the first login.
- After logging in to the SSL VPN, senior executives user_0001 can use the web proxy service. Click **Webmail** and **ERP** to use the corresponding services.



User Access Verification Configuration (2/3)

- In the upper right of the web UI, click **User Options** to download and install the client software. After setting SSL VPN parameters, senior executives can use the network extension function. The vNIC is automatically installed and the virtual IP address is obtained. You can use various services as if you were on a LAN.



User Access Verification Configuration (3/3)

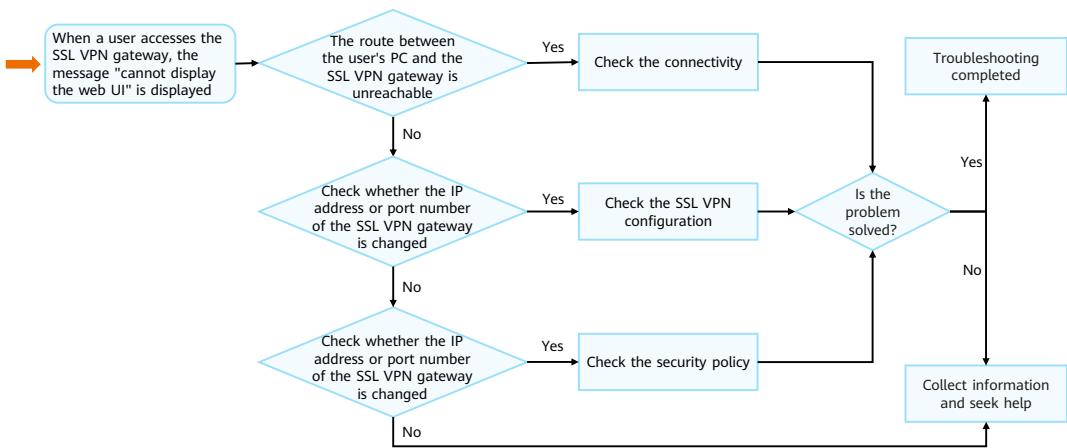
- Use common employee account **user_0002** to log in to the SSL VPN gateway. You can use only the web proxy service. You can click **Webmail** and **ERP** to use corresponding services.



Contents

1. Overview of SSL VPN
2. Service Functions of SSL VPN
3. Examples for Configuring the SSL VPN
- 4. SSL VPN Troubleshooting**

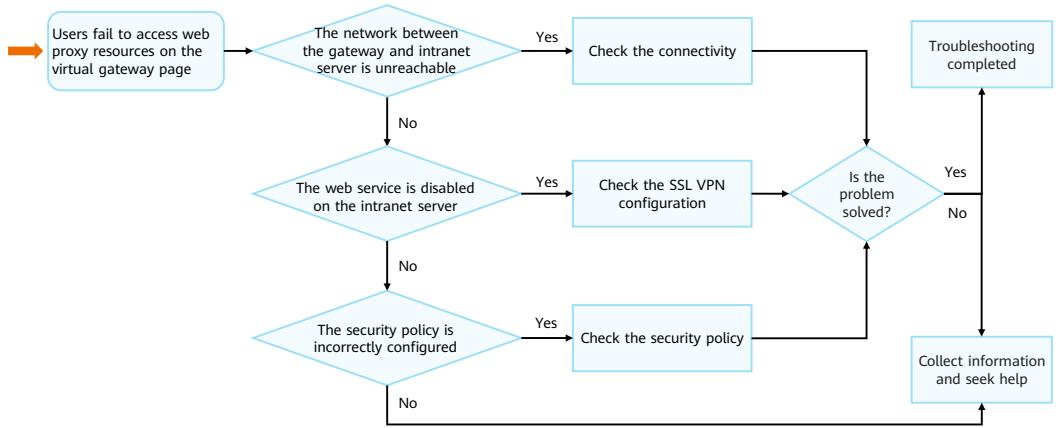
Displaying a Message that the Web UI Cannot Be Displayed



Procedure

- Diagnose the fault based on the preceding process.
 - The route between the user PC and the SSL VPN gateway is unreachable.
 - Run the **ping** command on the PC to test the connectivity to the IP address of the virtual gateway. If the ping operation fails, the route is unreachable. So, check the network status and ensure that the route is correctly configured.
 - The IP address or port number of the SSL VPN gateway has been changed.
 - Contact the administrator to obtain the correct SSL VPN gateway address and port number.
 - The security policy is incorrectly configured.
 - Log in to the web UI of the firewall as an administrator and choose **Policy > Security Policy > Security Policy** in the navigation pane.
 - Check the security policy configuration to determine which security policy restricts the user from logging in to the SSL VPN gateway. If so, modify the configuration of this policy.

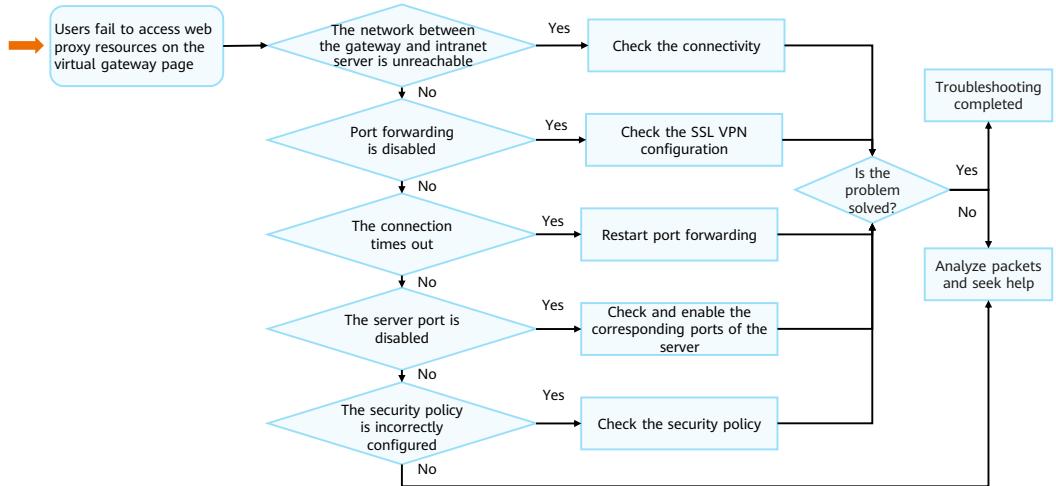
Failing to Access Web Proxy Resources



Procedure

- Diagnose the fault based on the preceding process.
 - The network between the gateway and intranet server is unreachable.
 - Log in to the firewall web UI as an administrator and choose **Monitor > Diagnosis Center** in the navigation pane. Select **Ping** and enter the IP address of the intranet server at the **Destination Host Name or IP Address** area. Click **Ping** to check the network connection.
 - If the ping operation fails, the network between the SSL VPN gateway and the intranet server is faulty. In this case, check the links between the gateway and intranet server. If the links are normal, check the routing configuration.
 - The web service is disabled on the intranet server.
 - If the route is reachable, choose **Start > Run** in the operating system of the intranet server. In the displayed dialog box, enter **cmd** and click **OK**.
 - Run the **netstat -anp tcp** command in the CLI to check whether the web service port is listening. If yes, the web service port is enabled. Otherwise, enable the web service port.
 - The security policy is incorrectly configured.
 - Log in to the web UI of the firewall as an administrator and choose **Policy > Security Policy > Security Policy** in the navigation pane.
 - Check the security policy configuration to determine which security policy restricts the user from logging in to the SSL VPN gateway. If so, modify the configuration of this policy.

Failing to Access Intranet Resources Through Port Forwarding



Procedure (1/2)

- Diagnose the fault based on the preceding process.
 - The network between the gateway and intranet server is unreachable.
 - Log in to the firewall web UI as an administrator and choose **Monitor > Diagnosis Center** in the navigation pane. Select **Ping** and enter the IP address of the intranet server in the **Destination Host Name or IP Address** area.
 - Click **Ping** to check the network connection. If the ping operation fails, the network between the SSL VPN gateway and the intranet server is faulty. In this case, check the links between the gateway and intranet server. If the links are normal, check the routing configuration.
 - If port forwarding is disabled:
 - Log in to the SSL VPN gateway page as a user. If the button under **Port Forwarding** is **Start**, port forwarding is not enabled. Click **Start** to enable port forwarding.
 - The connection times out:
 - After the user connection times out, the button under **Port Forwarding** changes to **Start**. Click **Start** to restart port forwarding. Then the login page is displayed. Log in again and enable port forwarding.

Procedure (2/2)

- The corresponding port is not enabled on the intranet server.
 - If the route is reachable, choose **Start > Run** in the operating system of the intranet server. In the displayed dialog box, enter **cmd** and click **OK**.
 - Run the **netstat -anp tcp** command in the CLI to check whether the service port is listening. If yes, the service port is enabled. Otherwise, enable the service port.
- The security policy is incorrectly configured.
 - Log in to the web UI of the case as an administrator and choose **Policy > Security Policy > Security Policy** in the navigation tree.
 - Check the security policy configuration to determine which security policy restricts the user access to the resource. If so, modify the configuration of this policy.

Quiz

1. (Single-answer question) A mobile user wants to access the internal file server of an enterprise, and user permissions need to be controlled in a refined manner. For example, common employees can access only common files. Which of the following SSL VPN functions can meet the preceding requirements? ()
 - A. Web proxy
 - B. File sharing
 - C. Port forwarding
 - D. Network extension

Summary

- This course describes the background of SSL VPN and the principles and application scenarios of its four functions (web proxy, file sharing, port forwarding, and network extension). Then this course lists the problems that network administrators may encounter during SSL VPN O&M and the troubleshooting roadmap.
- Upon completion of this course, you will be able to independently configure Huawei SSL VPN and deploy SSL VPN in the cyber security solution.

Recommendations

- Huawei Official Websites
 - Enterprise service: <https://e.huawei.com/en/>
 - Technical support: <https://support.huawei.com/enterprise/en/index.html>
 - Online learning: <https://www.huawei.com/en/learning>

Acronyms and Abbreviations (1/2)

Acronym/Abbreviation	Full Name
AD	Active Directory
ERP	Enterprise Resource Planning system
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IPsec	Internet Protocol Security
ISP	Internet Service Provider
NAT	Network Address Translation
NFS	Network File System
SIP	Session Initiation Protocol

Acronyms and Abbreviations (2/2)

Acronym/Abbreviation	Full Name
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell Protocol
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
telnet	Telecommunication Network Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VPN	Virtual Private Network

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。
Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

Copyright©2022 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product performance, market position, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.



Cyber Attacks and Defense



Foreword

- With the implementation of technologies and concepts such as cloud computing, big data, artificial intelligence (AI), and the Internet of Things (IoT), technological transformations take place in every corner of cyberspace and the real world. The changing technical and industrial environments have led to new generations of cyber attacks with higher intensity.
- Among multiple types of network attacks, DDoS attacks are one of the most common attacks because they are highly covert, destructive, and difficult to defend against. In addition, traditional single-packet attacks also cause great damage to networks and systems.
- This course describes the principles and defense technologies of common cyber attacks.

Objectives

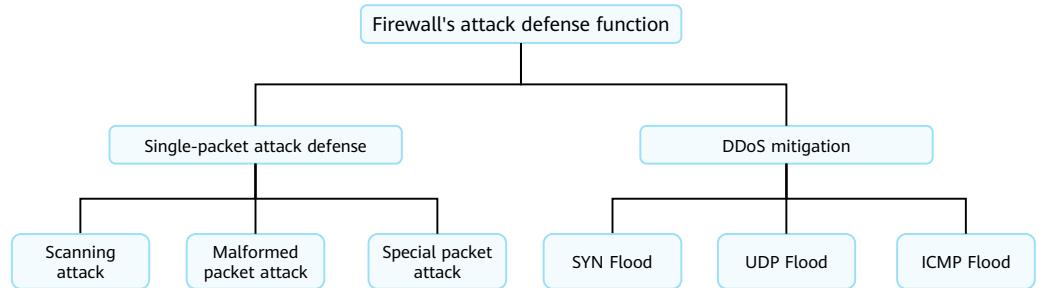
- Upon completion of this course, you will be able to:
 - Describe the principles of common single-packet attacks.
 - Describe the principles of common DDoS attacks.
 - Describe the principles of defending against single-packet attacks.
 - Describe the principles of defending against DDoS attacks.
 - Describe the anti-DDoS solution and related defense principles.

Contents

- 1. Firewall Attack Defense Technologies**
2. Single-Packet Attack Defense
3. DDoS Mitigation
4. Anti-DDoS

Introduction to Attack Defense Technologies

- With the attack defense function, firewalls can detect various cyber attacks, protect the intranet from malicious attacks, and ensure the normal running of the intranet hosts.
- The attack defense function can defend against traditional single-packet attacks and various common DDoS attacks.



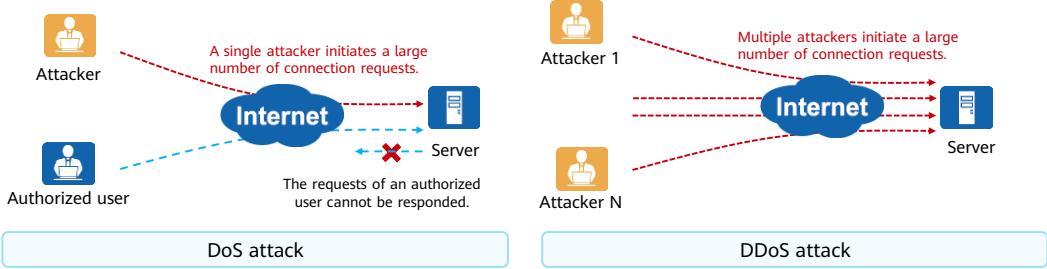
Single-Packet Attack

- Single-packet attacks are categorized as scanning attacks, malformed packet attacks, and special packet attacks.

Scanning attack	Malformed packet attack	Special packet attack
<ul style="list-style-type: none">• Scanning attacks are potential attack behaviors that do not directly cause damages. They are typically used for network detection before the real attacks.• Examples of such attacks include IP sweep attack and port scan attack.	<ul style="list-style-type: none">• Attackers send considerable malformed packets in an attempt to crash targeted hosts or servers.• Examples of such attacks include Ping of Death attacks, Smurf attacks, Fraggle attacks, and local area network denial (LAND) attacks.	<ul style="list-style-type: none">• Special packet attacks are potential attack behaviors that do not directly cause damages. Attackers use special control packets to probe network structures before subsequent real attacks.• Examples of such attacks include ICMP redirect attacks and Tracert attacks.

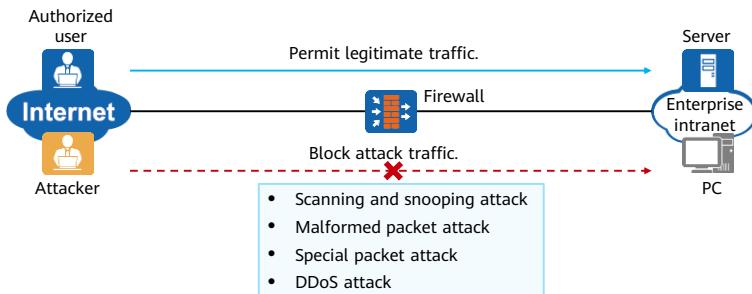
DDoS Attack

- DDoS attacks are distributed denial of service (DoS) attacks. DoS attacks exploit TCP/IP defects to occupy protocol stack resources or congest the links through heavy traffic, degrading the performance or consuming the bandwidth resources of the target host. Different from other attack methods of leaving Trojan horses and backdoors or hijacking data on a host, DoS attacks cause no harm to sensitive data. However, they block authorized user access to required services.
- Based on DoS attacks, multiple computers are combined as an attack platform to launch DDoS attacks on one or more targets. This multiplies the attack damage, making the target server unable to provide normal services.



Application Scenarios of Attack Defense Technologies

- Generally, a firewall is deployed at the egress of an enterprise intranet. After the attack defense function is enabled, the firewall can distinguish between legitimate traffic and attack traffic, permit legitimate traffic, and block attack traffic. This effectively ensures the normal running of enterprise intranet server and PCs.



Contents

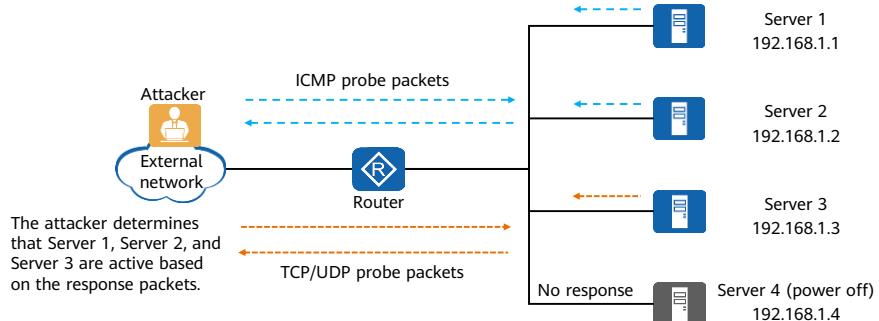
1. Firewall Attack Defense Technologies
2. **Single-Packet Attack Defense**
 - Principles of Single-Packet Attack Defense
 - Configuration of Single-Packet Attack Defense
3. DDoS Mitigation
4. Anti-DDoS

Common Single-Packet Attacks

Scanning attacks	Malformed packet attacks	Special packet attacks
IP sweep attack Port scan attack	Smurf attack LAND attack Fraggle attack IP fragment attack IP spoofing attack Ping of Death attack TCP flag attack Teardrop attack	Large ICMP packet attack ICMP redirect attack ICMP unreachable packet attack Tracert packet attack IP source route option attack IP route record option attack IP timestamp option attack

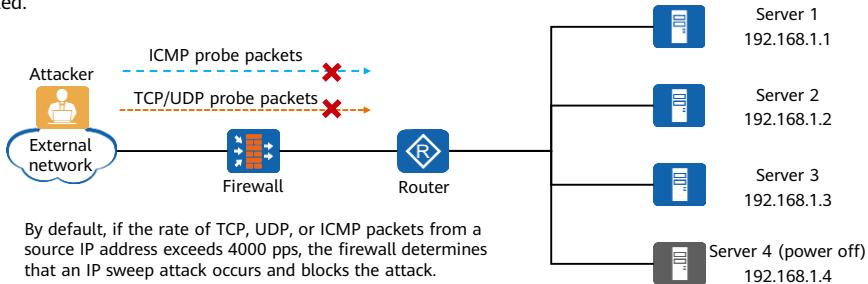
Principles of the IP Sweep Attack

- Attackers use ICMP packets (for example, the **ping** or **tracert** command) to probe target IP addresses or use TCP/UDP packets (for example, TCP ping) to initiate connections to certain IP addresses. If a response packet from an IP address is received, the attacker can know that the corresponding target system is active.



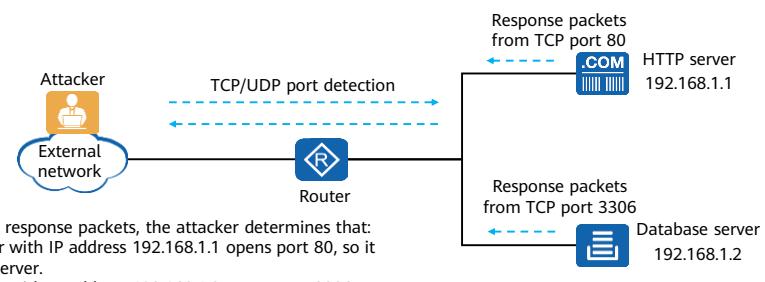
Principles of IP Sweep Attack Defense

- After IP sweep attack defense is configured, the firewall detects the received TCP, UDP, and ICMP packets. If the number of packets sent from a specific source IP address to different destination IP addresses per second exceeds the preset threshold, the firewall determines that the host at this source IP address launches IP sweep attacks and blacklists this IP address.
- IP sweep attack defense collects the rate of the first IP packet, and detects a source IP address that is not whitelisted.



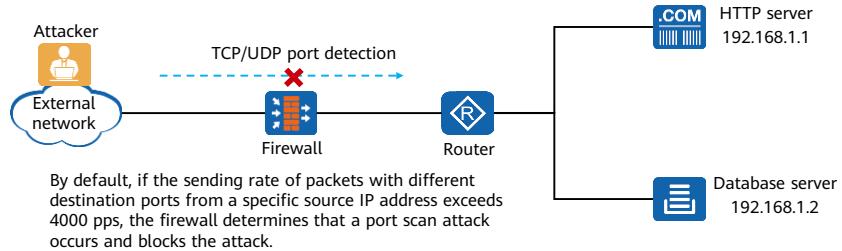
Principles of the Port Scan Attack

- An attacker scans ports to identify open ports on the attack target and thereby determines the attack method. The attacker usually uses the port scanning software to initiate connections to a series of TCP or UDP ports on a wide range of hosts. Based on the response packets, the attacker can determine whether the hosts use these ports for providing services.



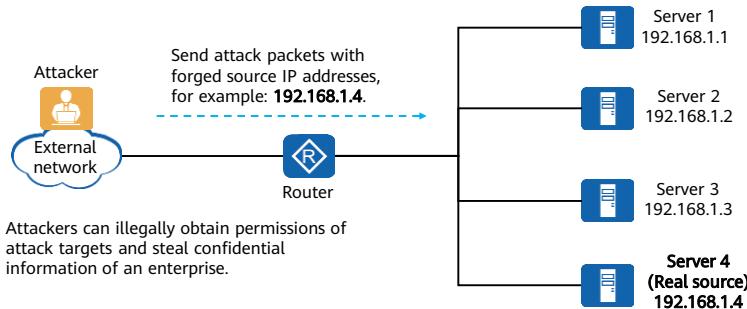
Principles of Port Scan Attack Defense

- After port scan attack defense is configured, the firewall detects the received TCP and UDP packets. If the number of packets with different destination ports from a specific source IP address per second exceeds the preset threshold, the firewall determines that the host at this IP address launches port scan attacks and blacklists this IP address.
- Port scan attack defense collects the rate of the first IP packet, and detects a source IP address that is not whitelisted.



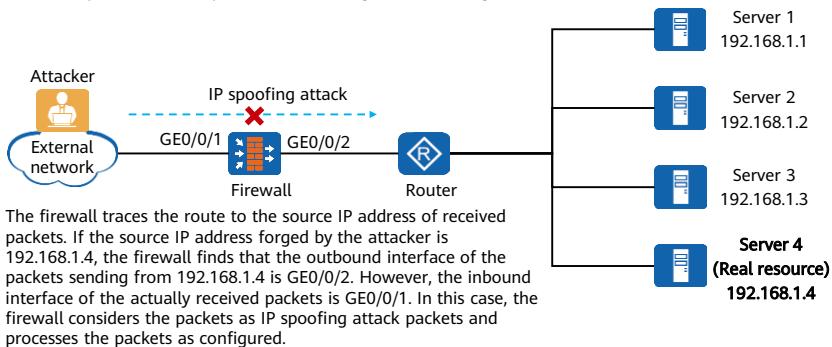
Principles of the IP Spoofing Attack

- IP spoofing attack is a commonly used attack type and is the basis of other types of attacks. In an IP spoofing attack, an attacker sends packets with forged source IP addresses to the target hosts to obtain superior access and control permissions, endangering target host resources and causing information leaks.



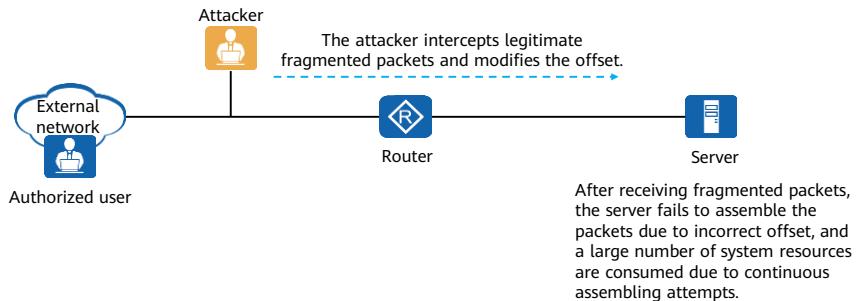
Principles of IP Spoofing Attack Defense

- After IP spoofing attack defense is enabled, the firewall traces the route to the source IP address of received packets and checks whether the outbound interface corresponding to the source IP address in the routing table is the same as the inbound interface of each packet. If they are different, the firewall considers the packets as IP spoofing attack packets and processes the packets according to the configured action.



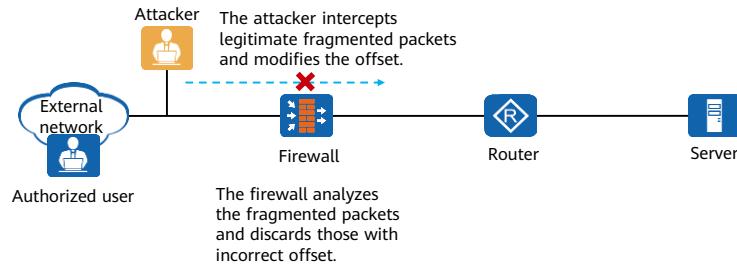
Principles of the Teardrop Attack

- Because the size of data transmitted at the link layer is limited by the maximum transmission unit (MTU), some large IP packets need to be fragmented during transmission. The fragmented packets carry the fragment flag bit and fragment offset in the IP header. If an attacker intercepts fragmented packets and modifies the offset, the data receiver cannot assemble the fragmented packets into a complete packet. As such, the receiver will keep trying to assemble the packets, therefore a large number of system resources are consumed.



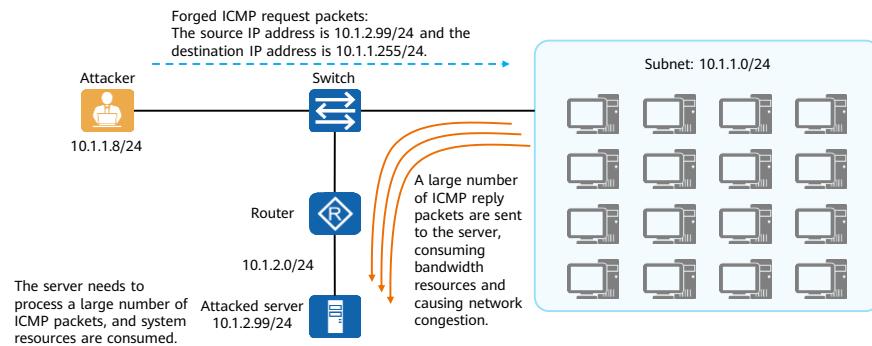
Principles of Teardrop Attack Defense

- After Teardrop attack defense is enabled, the firewall analyzes received fragmented packets and checks whether the fragment offset is correct. If not, the firewall discards the packets and logs the attack.



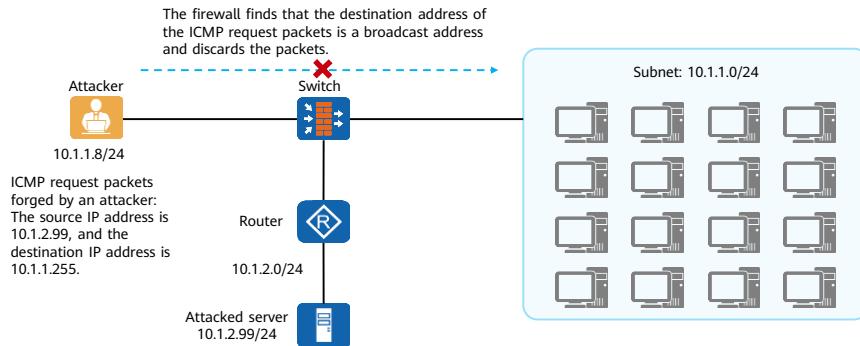
Principles of the Smurf Attack

- Attackers do not directly attack the target server. Instead, they forge a large number of ICMP request packets to launch cyber attacks. Attackers send packets with the source IP address being the IP address of attacked server, and the destination address being the broadcast address of a network. As a result, numerous hosts send ICMP reply packets to the attacked server. In this way, network bandwidth and system resources of the server are consumed. Such attacks are called Smurf attacks.



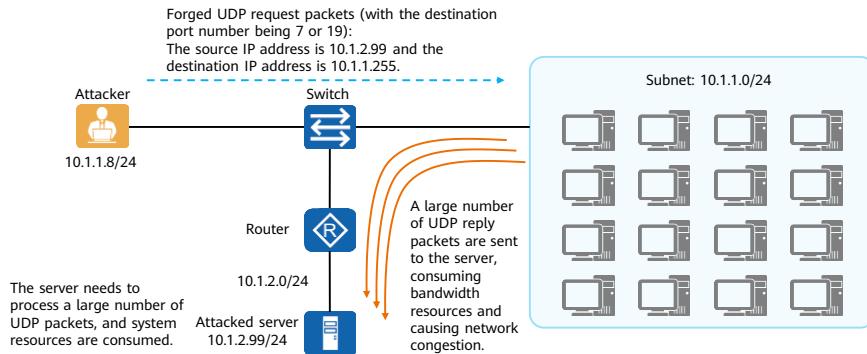
Principles of Smurf Attack Defense

- After the Smurf attack defense is enabled, the firewall checks whether the destination address of the ICMP request packets is a broadcast address (that is, the host bits are all 1) or a network address (that is, the host bits are all 0). If so, the firewall discards the packets and logs the attack.



Principles of the Fraggle Attack

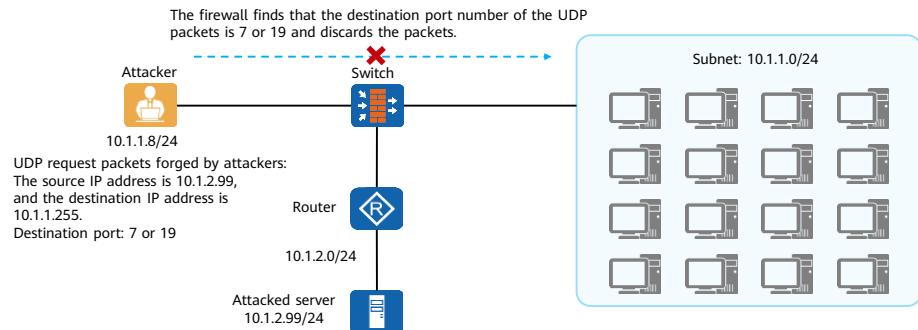
- The principles of the Fraggle attack are similar to those of the Smurf attack. Attackers forge a large number of UDP request packets with the destination port number being 7 or 19 to launch cyber attacks. The packets' source IP address is the IP address of attacked server, and the destination address is the broadcast address of a network. As a result, a large number of hosts in the network send UDP reply packets to the attacked server. In this way, network bandwidth and system resources of the server are consumed. Such attacks are called Fraggle attacks.



- UDP port 7 is a well-known port that corresponds to the Echo protocol. After receiving a UDP Echo request packet, the host responds with a packet containing the same content.
- UDP port 19 is a well-known port that corresponds to the Chargen protocol. After receiving a UDP Chargen request packet, the host responds with a packet containing a character string.

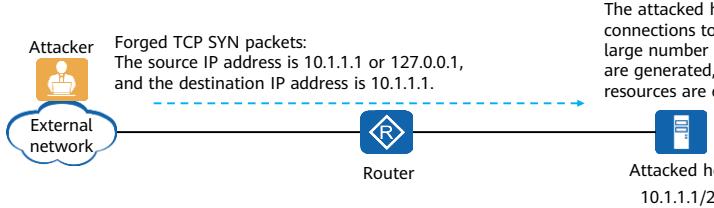
Principles of Fraggle Attack Defense

- After the Fraggle attack defense is enabled, the firewall detects received UDP packets. If the destination port number of a packet is 7 or 19, the firewall rejects the packet and logs the attack.



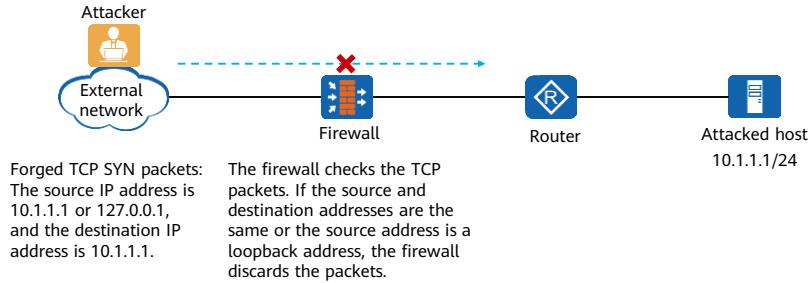
Principles of the LAND Attack

- An attacker sends forged TCP SYN packets to a target host. The source and destination addresses of the forged packets are the same or the source address is a loopback address (127.0.0.0/8). As a result, the target host sends SYN-ACK messages to its own IP address. Therefore, a large number of TCP null connections are generated and system resources are consumed. This type of attack is called the LAND attack or loopback attack.



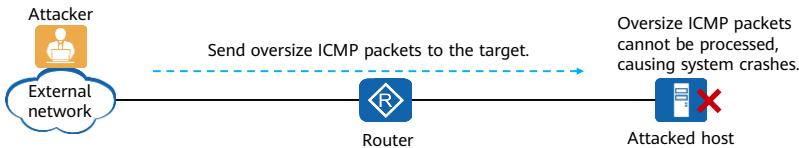
Principles of LAND Attack Defense

- After the Land attack (loopback attack) defense is enabled, the firewall checks whether the source and destination addresses of TCP packets are the same, or the source address of TCP packets is a loopback IP address. If so, the firewall discards the packets and logs the attack.



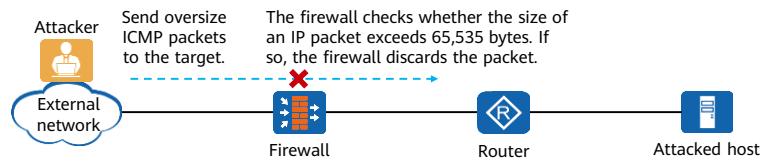
Principles of the Ping of Death Attack

- The length field of an IP packet is 16 bits, indicating that the maximum length of an IP packet is 65535 bytes. Ping of Death attacks intrude a system by sending oversized ICMP packets.
- Some systems or devices cannot process oversize ICMP packets. After receiving such packets, the systems may crash, break down, or restart.



Principles of Ping of Death Attack Defense

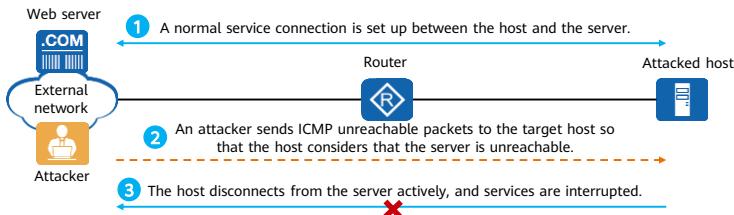
- After the Ping of Death attack defense is enabled, the firewall checks whether the packet size is larger than 65,535 bytes. If a packet is larger than 65,535 bytes, the firewall discards the packet and logs the attack.



- The firewall can also defend against oversize ICMP packets that do not exceed 65535 bytes. You can define the maximum length of permitted ICMP packets based on network requirements. If the firewall detects that the actual length of ICMP packets exceeds the threshold, it considers that an oversize ICMP packet attack occurs, and then discards the packets.

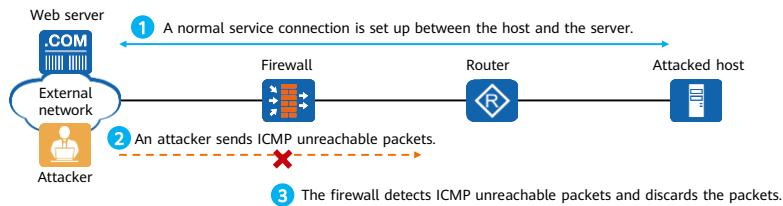
Principles of ICMP Unreachable Attack

- Different systems process ICMP unreachable packets in different ways. After receiving an ICMP unreachable packet from a network or host, some systems consider subsequent packets destined for this destination IP address unreachable and disconnect normal service connections. An attacker exploits this vulnerability by forging ICMP unreachable packets, causing the target system to terminate the connection with the destination.



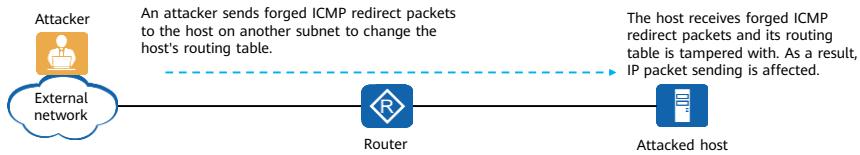
Principles of ICMP Unreachable Attack Defense

- After ICMP unreachable attack defense is enabled, the firewall discards ICMP unreachable packets and logs the attack.



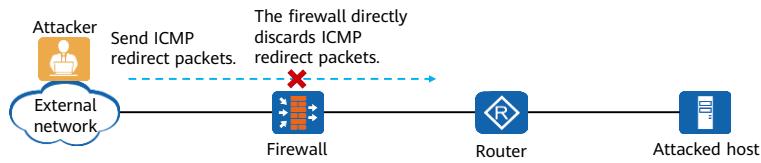
Principles of the ICMP Redirect Attack

- A network device sends ICMP redirect packets to hosts on the same subnet, requesting the hosts to change the routes. Generally, a device sends ICMP redirect packets only to hosts on the same subnet. However, some malicious attackers may send forged ICMP redirect packets to hosts on another subnet to change the routing tables of the hosts, disabling the hosts from forwarding IP packets.



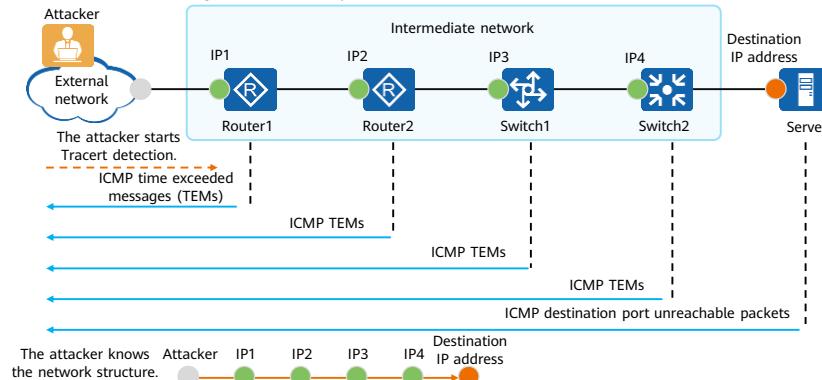
Principles of ICMP Redirect Attack Defense

- After ICMP redirect attack defense is enabled, the firewall discards all received ICMP redirect packets and logs the attack.



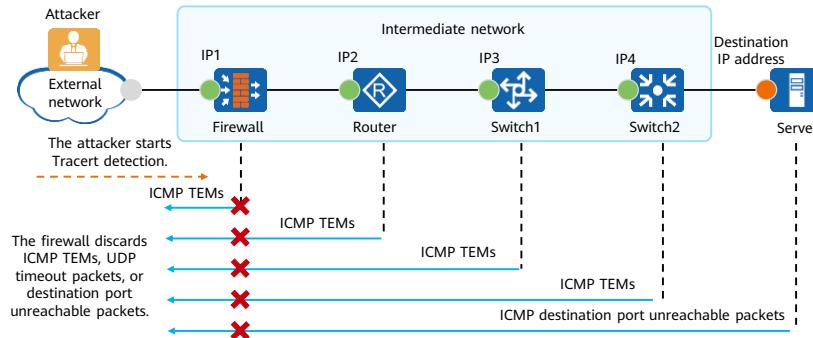
Principles of the Tracert Attack

- In a Tracert attack, an attacker discovers the packet transmission path using the ICMP timeout packets returned when the Time To Live (TTL) value is 0 and ICMP port unreachable packets returned when the packet reaches the destination IP address. In this way, the attacker probes the network structure.



Principles of Tracert Attack Defense

- After the Tracert attack defense is enabled, the firewall discards ICMP TEMs, UDP timeout packets, or destination port unreachable packets, and logs the attack.



Contents

1. Firewall Attack Defense Technologies
2. **Single-Packet Attack Defense**
 - Principles of Single-Packet Attack Defense
 - Configuration of Single-Packet Attack Defense
3. DDoS Mitigation
4. Anti-DDoS

Configuration of IP Sweep Attack Defense

- Configuring IP sweep attack defense

- Enable IP sweep attack defense.

```
[FW] firewall defend ip-sweep enable
```

- Set the threshold for the IP address sweep rate. If the sweep rate of a host exceeds the threshold, the host is considered as an attacker's device.

```
[FW] firewall defend ip-sweep max-rate max-rate-number
```

- Set the action for defending against single-packet attacks to **discard**.

```
[FW] firewall defend action discard
```

- Enable the blacklist function. The attacker's IP address is blacklisted after being identified.

```
[FW] firewall blacklist enable
```

```
[FW] firewall defend ip-sweep blacklist-timeout interval
```

- After IP sweep attack defense is configured, the firewall detects the received TCP, UDP, and ICMP packets. If the number of packets sent from a specific IP address to different destination IP addresses per second exceeds the preset threshold, the firewall determines that the host at this IP address launches IP sweep attacks and takes either of the following actions on the source IP address:
 - If the blacklist function is enabled and the **firewall defend action discard** command is configured on the firewall, the firewall blacklists the source IP address and discards the packets sent from this IP address.
 - If the blacklist function is disabled but the **firewall defend action discard** command is configured on the firewall, the firewall generates alarms and discards the packets sent from this IP address.
- If a source IP address is whitelisted, IP sweep attack defense will not be implemented on the source IP address.

Configuration of Port Scan Attack Defense

- Configuring port scan attack defense

- Enable port scan attack defense.

```
[FW] firewall defend port-scan enable
```

- Configure the threshold for the port scan rate. If the port scan rate of a host exceeds the threshold, the host is considered as an attacker's device.

```
[FW] firewall defend port-scan max-rate max-rate-number
```

- Set the action for defending against single-packet attacks to **discard**.

```
[FW] firewall defend action discard
```

- Enable the blacklist function. The attacker's IP address is blacklisted after being identified.

```
[FW] firewall blacklist enable
```

```
[FW] firewall defend port-scan blacklist-timeout interval
```

- After port scan attack defense is configured, the firewall detects the received TCP and UDP packets. If the number of packets with different destination ports from a specific source IP address per second exceeds the preset threshold, the firewall determines that the host at this IP address launches port scan attacks and takes either of the following actions on the source IP address:
 - If the blacklist function is enabled and the **firewall defend action discard** command is configured on the firewall, the firewall blacklists the source IP address and discards the packets sent from this IP address.
 - If the blacklist function is disabled but the **firewall defend action discard** command is configured on the firewall, the firewall generates alarms and discards the packets sent from this IP address.
- If a source IP address is whitelisted, port scan attack defense will not be implemented on the source IP address.

Configuration of Single-Packet Attack Defense (1/2)

- Configure IP spoofing attack defense.

```
[FW] firewall defend ip-spoofing enable
```

- Configure Teardrop attack defense.

```
[FW] firewall defend teardrop enable
```

- Configure Smurf attack defense.

```
[FW] firewall defend smurf enable
```

- Configure Land attack defense.

```
[FW] firewall defend land enable
```

- Configure Fraggle attack defense.

```
[FW] firewall defend fraggle enable
```

- Configure Ping of Death attack defense.

```
[FW] firewall defend ping-of-death enable
```

Configuration of Single-Packet Attack Defense (2/2)

- Configure oversize ICMP packet attack defense.

```
[FW] firewall defend large-icmp enable  
[FW] firewall defend large-icmp max-length length
```

- Configure ICMP unreachable attack defense.

```
[FW] firewall defend icmp-unreachable enable
```

- Configure ICMP redirect attack defense.

```
[FW] firewall defend icmp-redirect enable
```

- Configure Tracert packet attack defense.

```
[FW] firewall defend tracert enable
```

Contents

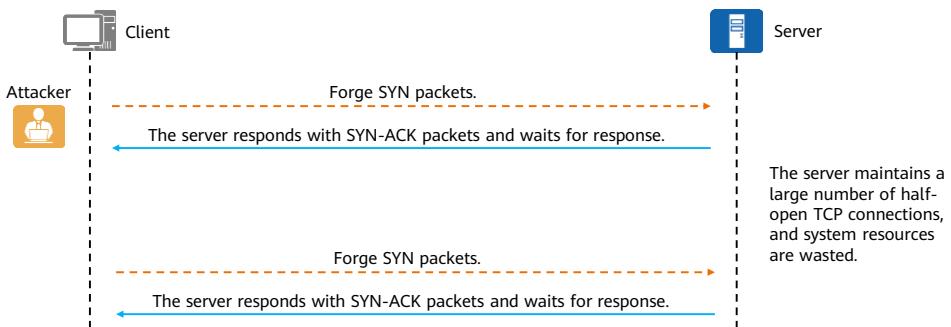
1. Firewall Attack Defense Technologies
2. Single-Packet Attack Defense
- 3. DDoS Mitigation**
 - Principles of DDoS Mitigation
 - Configuration of DDoS Mitigation
4. Anti-DDoS

Introduction to DDoS Mitigation Technologies

Technology	Principle	Applicable Attack Types
Source IP address detection	The firewall detects the source IP address of a request packet. If the source IP address is a real IP address, the firewall forwards the packet; otherwise, the firewall discards the packet.	SYN flood, HTTP flood, HTTPS flood, DNS request flood, DNS reply flood, and SIP flood
Fingerprint	The firewall learns the characteristics of detected attack packets and saves them as fingerprints. If a packet matches a fingerprint, the firewall discards the packet; otherwise, the firewall forwards the packet.	UDP flood and UDP fragment flood
Traffic limiting	Once the rate of packets exceeds the threshold, the firewall discards the packets.	ICMP flood, UDP flood

Principles of the SYN Flood Attack

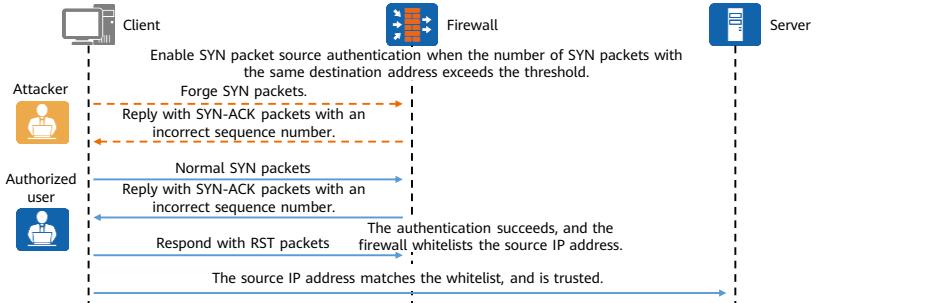
- An attacker forges a large number of SYN request packets and sends them to the server. The server responds with a SYN-ACK packet each time it receives a SYN packet. However, the attacker ignores the SYN-ACK packet. As a result, a large number of half-open TCP connections exist on the server, and maintaining these connections consumes a large number of CPU and memory resources. Therefore, the server has no time to process normal SYN requests and rejects services for authorized users. Such attacks are called SYN flood attacks.



- The principles of FIN flood attacks, RST flood attacks, and ACK flood attacks are similar to that of SYN flood attacks. They are launched by exploiting forged TCP packets with special flag bits. As a result, the target server's system resources are consumed, causing denial of normal services. The details of these attacks are not provided here.

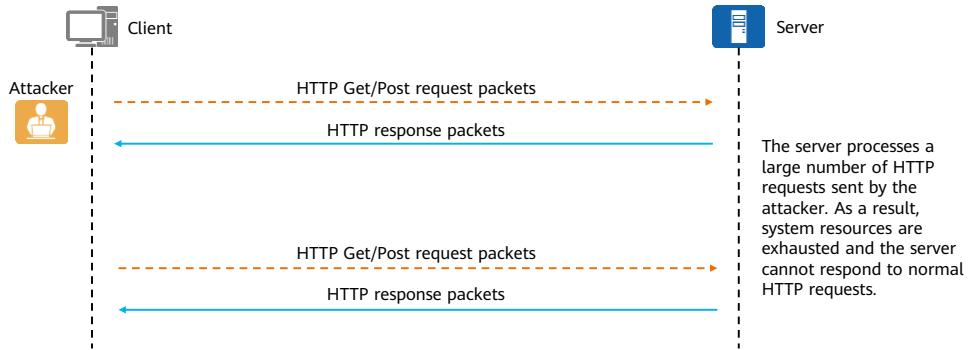
Principles of SYN Flood Attack Defense

- If the number of SYN packets with the same destination IP address received by the firewall within a period of time exceeds the threshold, SYN packet source authentication is triggered. The firewall intercepts the SYN packets, forges SYN-ACK packets with an incorrect sequence number, and sends the packets to the client.
 - If the source IP address is forged, the client does not respond to the incorrect SYN-ACK packets. As a result, the authentication fails, and the firewall discards subsequent SYN packets sent from this source IP address.
 - If the source IP address is real, the client responds with RST packets. As a result, the authentication succeeds, and the firewall whitelists the source IP address and permits subsequent SYN packets.



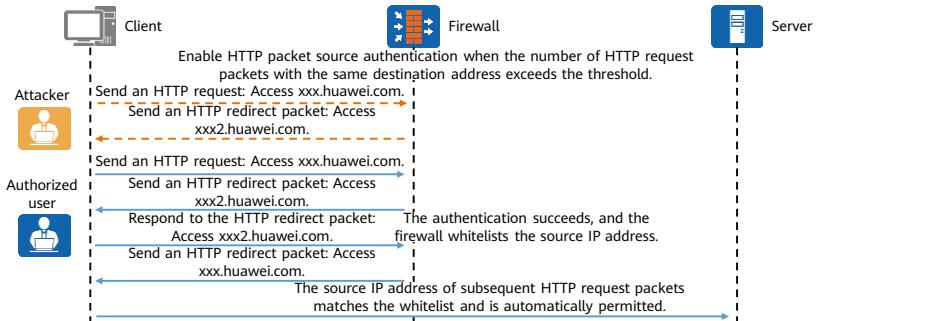
Principles of the HTTP Flood Attack

- An attacker sends a large number of HTTP Get or HTTP Post request packets to the target server through proxies or zombie hosts. These request packets (for example, database operation requests) generally consume a large number of server system resources. As a result, the server system resources are exhausted and the server cannot respond to normal requests. Such attacks are called HTTP flood attacks.



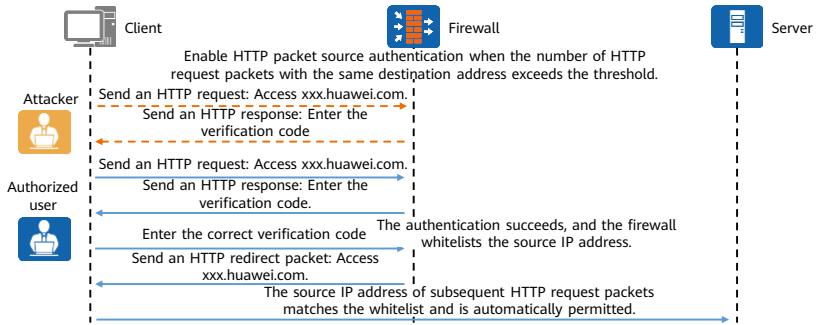
Principles of HTTP Flood Attack Defense (Basic Mode)

- If the number of HTTP request packets with the same destination address received by the firewall within a period of time exceeds the threshold, HTTP packet source authentication is triggered. The firewall intercepts the HTTP request packets and sends HTTP redirect packets to the client.
 - If the source IP address is forged, the client does not respond to the HTTP redirect packets. As a result, the authentication fails, and the firewall discards subsequent HTTP request packets from this source IP address.
 - If the source IP address is real, the client responds to the HTTP redirect packets. As a result, the authentication succeeds, the source IP address is whitelisted, and subsequent HTTP request packets are automatically permitted.



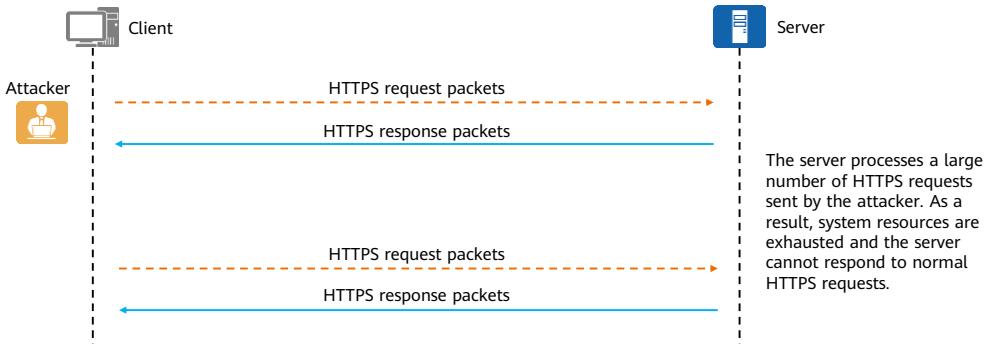
Principles of HTTP Flood Attack Defense (Enhanced Mode)

- If the number of HTTP request packets with the same destination address received by the firewall within a period of time exceeds the threshold, HTTP packet source authentication is triggered. The firewall intercepts the HTTP request packets, responds the client with an HTTP page, and requests the user to enter the verification code on the page.
 - If the source IP address is forged, no verification code will be entered and the authentication fails. The firewall discards subsequent HTTP request packets from this source IP address.
 - If the source IP address is real, the user will enter the correct verification code. As a result, the authentication succeeds, the source IP address is added to the firewall whitelist, and subsequent HTTP request packets are automatically permitted.



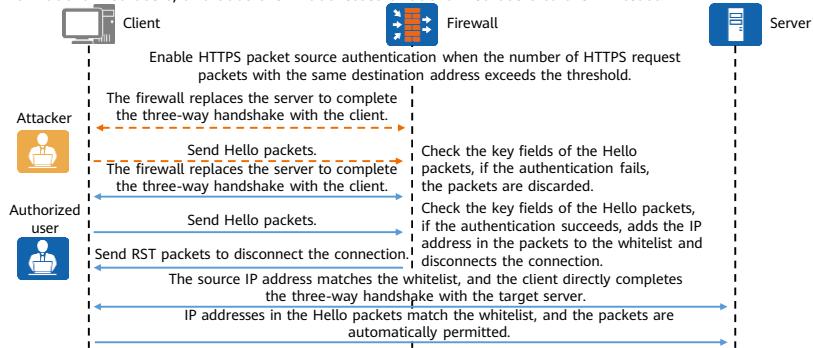
Principles of the HTTPS Flood Attack

- Attackers launch a large number of HTTPS connections to the target server directly or through proxies or zombies. As a result, the server is overloaded and unable to respond to authorized requests. Such attacks are called HTTPS flood attacks.



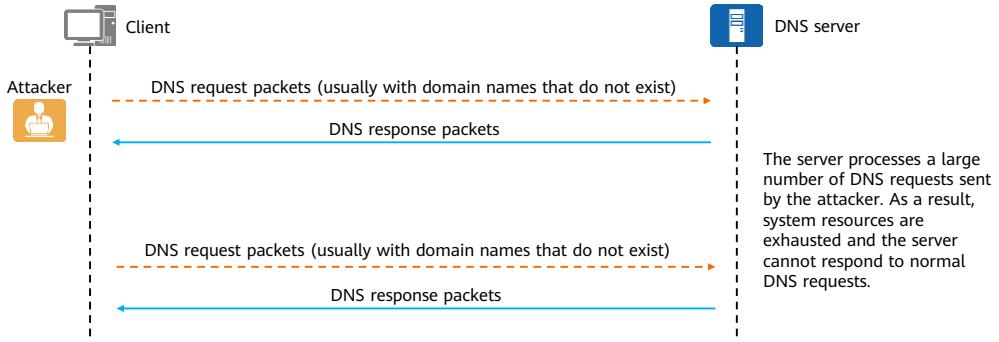
Principles of HTTPS Flood Attack Defense

- The firewall collects rate statistics on HTTPS packets (request and response packets) destined for port 443 based on destination addresses. When the rate of HTTPS packets whose destination addresses are the same and the destination ports are all 443 reaches the threshold, source authentication is triggered. The firewall completes the three-way handshake with the client on behalf of the server. Then, the firewall checks the key fields of the Hello packets sent by the client, discards the packets from the attacker, permits the packets from authorized users, and adds the IP addresses of authorized users to the whitelist.



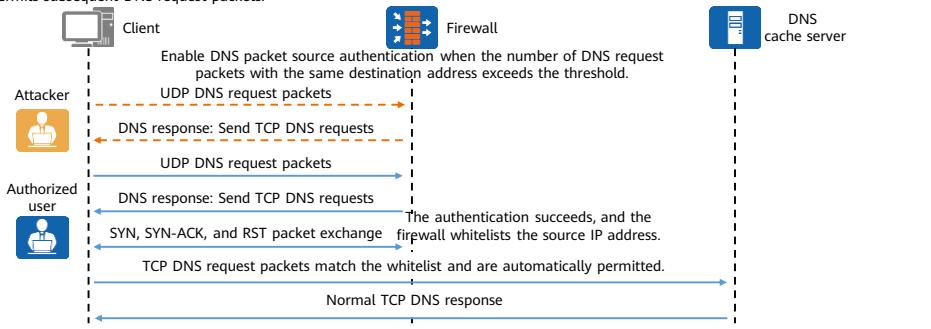
Principles of the DNS Request Flood Attack

- An attacker sends a large number of domain name (usually non-existent) resolution requests to the DNS server. As a result, a large number of DNS cache server or authoritative server system resources are consumed, and the server breaks down and cannot respond to normal DNS requests. Such attacks are called DNS request flood attacks.



Principles of DNS Request Flood Attack Defense (for the DNS Cache Server)

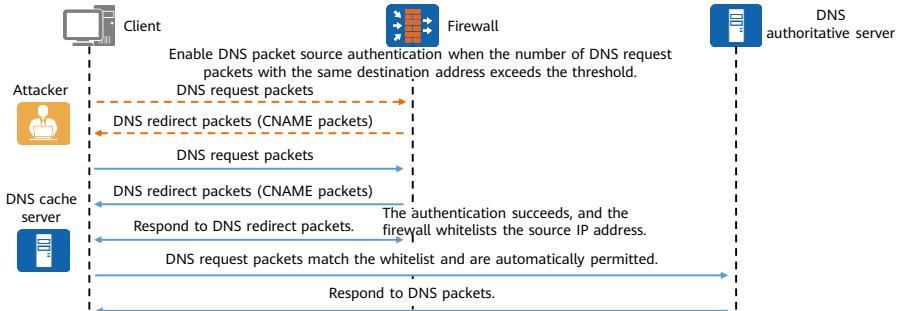
- If the number of DNS request packets with the same destination address received by the firewall within a period of time exceeds the threshold, DNS packet source authentication is triggered. The firewall requires the client to send TCP DNS requests.
 - If the source IP address is forged, the client does not send TCP DNS requests. As a result, the authentication fails, and the firewall rejects subsequent DNS request packets sent from this IP address.
 - If the source IP address is real, the client sends TCP DNS requests. After the authentication succeeds, the client's IP address is whitelisted and the firewall permits subsequent DNS request packets.



- During DNS source authentication, the firewall instructs the client to send TCP DNS request packets to check the validity of source IP addresses, which consumes the DNS cache server's TCP connection resources.
- Source authentication in this mode effectively defends against DNS request attacks on the DNS cache server. However, this mode does not apply to all scenarios on live networks because not all clients can send TCP DNS requests. If a client cannot send TCP DNS requests, this source authentication mode will affect normal services.

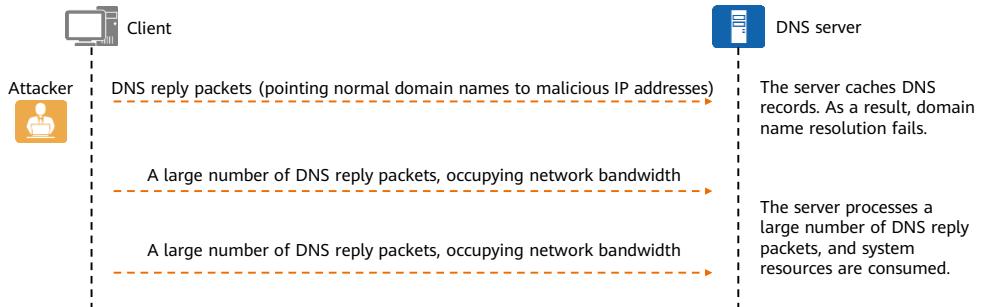
Principles of DNS Request Flood Attack Defense (for the DNS Authoritative Server)

- If the number of DNS request packets with the same destination address received by the firewall within a period of time exceeds the threshold, DNS packet source authentication is triggered. The firewall sends DNS redirect packets to the client:
 - If the source IP address is forged, the client does not respond to DNS redirect packets. As a result, the authentication fails, and the firewall rejects subsequent DNS request packets.
 - If the source IP address is real, the client responds to the DNS redirect packets. As a result, the authentication succeeds. The firewall adds the source IP address to the whitelist, and permits subsequent DNS request packets.



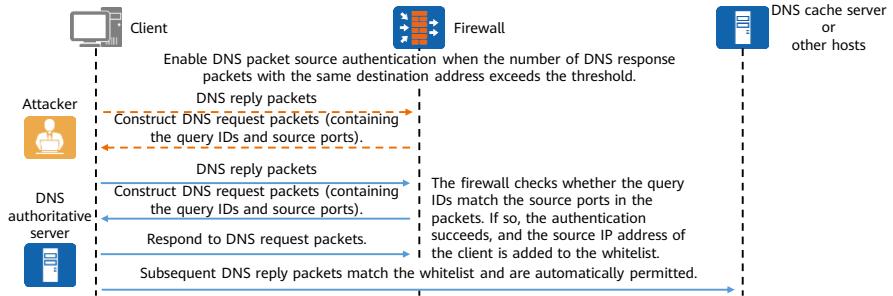
Principles of the DNS Reply Flood Attack

- An attacker sends a large number of DNS reply packets to the DNS server to consume server resources. Such attacks are called DNS reply flood attacks, which may have the following impacts:
 - DNS reply packets point normal domain names to malicious IP addresses, affecting normal DNS resolution.
 - A large number of DNS reply packets consume bandwidth resources and server system resources. As a result, the DNS server breaks down and cannot provide normal services.



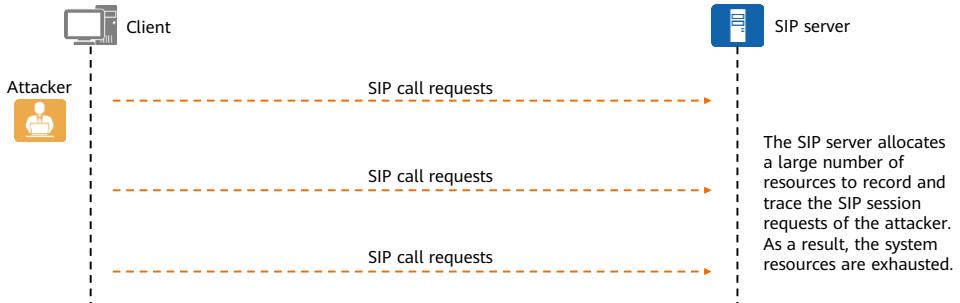
Principles of DNS Reply Flood Attack Defense

- If the number of DNS response packets with the same destination address received by the firewall within a period of time exceeds the threshold, DNS packet source authentication is triggered. The firewall constructs new DNS request packets (containing the query IDs and source ports) and sends them to the source client.
 - If the source IP address is forged, the client does not respond to the DNS request packets. As a result, the authentication fails and the firewall rejects the DNS response packets.
 - If the source IP address is real, the client responds to the DNS request packets. As a result, the authentication succeeds. The firewall adds the source IP address to the whitelist, and permits subsequent DNS response packets.



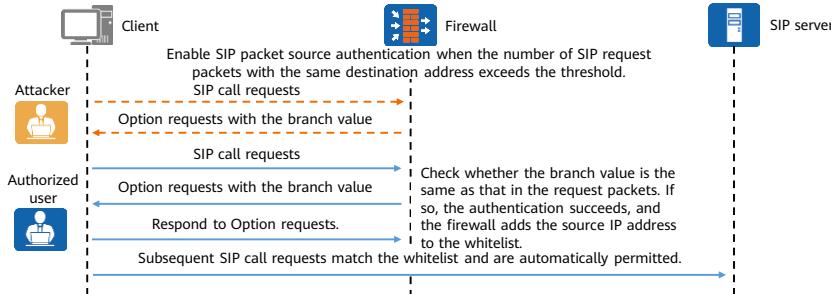
Principles of the SIP Flood Attack

- An attacker sends a large number of SIP call requests to the SIP server. The SIP server allocates a large number of resources to record and trace the sessions. As a result, the system resources are exhausted and the SIP server cannot respond to the call requests of authorized users. Such attacks are called SIP flood attacks.



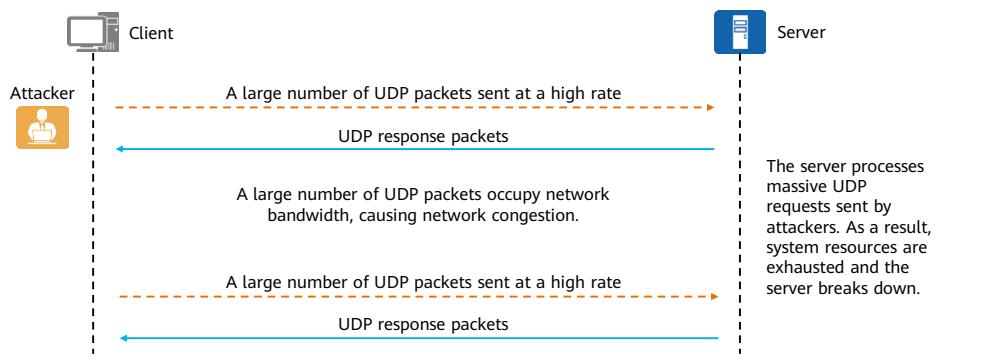
Principles of SIP Flood Attack Defense

- If the number of SIP request packets with the same destination address received by the firewall within a period of time exceeds the threshold, SIP packet source authentication is triggered. The firewall sends Option request packets containing the branch value to the source client.
 - If the source IP address is forged, the client does not respond to the Option requests. As a result, the authentication fails, and the firewall rejects the subsequent SIP request packets.
 - If the source IP address is real, the client responds to the Option requests. As a result, the authentication succeeds. The firewall adds the source IP address to the whitelist, and permits subsequent SIP response packets.



Principles of the UDP Flood Attack

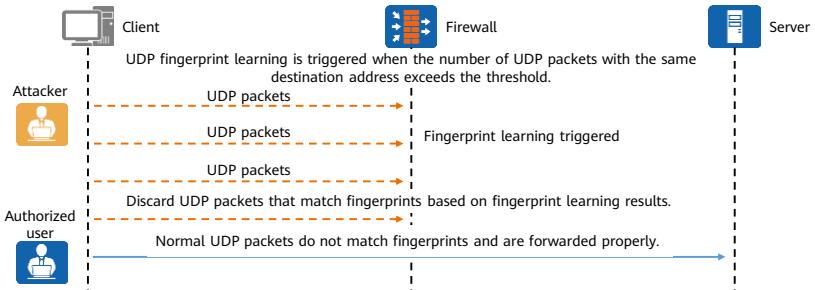
- UDP provides connectionless services. An attacker sends a large number of UDP packets to a server, for example, the DNS server, RADIUS authentication server, or streaming media video server. As a result, the server bandwidth and system resources are exhausted and the server cannot provide services properly. Such attacks are called UDP flood attacks.



- UDP flood attacks are classified into small packet attacks and large packet attacks.
 - A small packet is a 64-byte packet, which is the minimum size of a data frame transmitted on the Ethernet. For the same volume of traffic, the smaller the size of a single packet, the larger the number of data packets. Network devices such as switches and routers need to check and verify each data packet. Therefore, small UDP packet attacks can effectively increase the pressure of network devices to process data packets, resulting in DoS attack effects (slow processing speed and transmission delay).
 - A large packet is a packet larger than 1500 bytes, which exceeds the size of the MTU of the Ethernet frames. A large UDP packet attack can effectively occupy the transmission bandwidth of the network interface and force the attacked target to fragment and reassemble the received UDP data. As a result, the network is congested and the server responds slowly.
- The principles of UDP fragment flood attacks are similar to that of UDP flood attacks, and are not mentioned here.

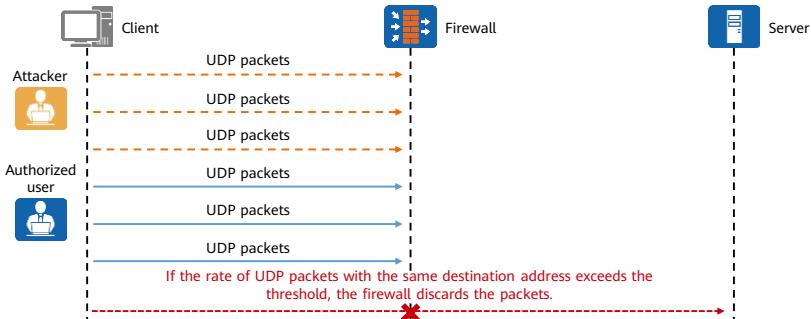
Principles of UDP Flood Attack Defense (Fingerprint Learning)

- UDP flood attack packets feature same characteristic fields. Firewalls can defend against UDP flood attacks through fingerprint learning.
- If the number of UDP packets with the same destination address received by the firewall within a period of time exceeds the threshold, fingerprint learning is triggered. The firewalls dynamically generate fingerprints based on the characteristics of attack packets and then discard the packets matching the fingerprints.



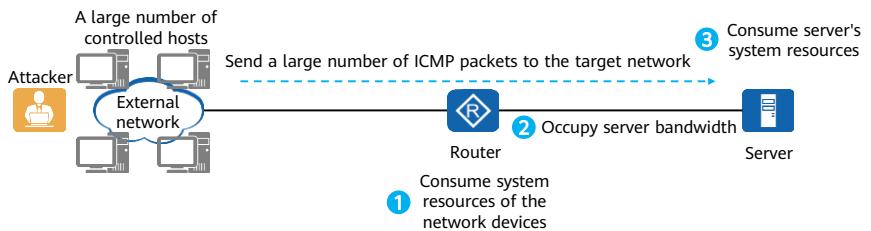
Principles of UDP Flood Attack Defense (Traffic Limiting)

- If fingerprint learning fails to defend against UDP flood attacks, you can use the traffic limiting technology. The traffic limiting technology sets a sending rate threshold of UDP packets destined for the same destination address and discards the packets whose rate exceeds the threshold to prevent network congestion.
- Traffic limiting cannot distinguish normal packets from attack packets and may affect normal services. Therefore, UDP fingerprint learning is recommended.



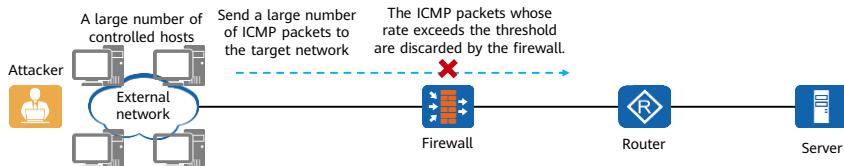
Principles of the ICMP Flood Attack

- In an ICMP flood attack, an attacker controls a large number of hosts and sends abundant oversized ICMP packets to the attack target in a short period of time. As a result, the network bandwidth and system resources of the target are occupied, resources are exhausted, and services are unavailable.
- Such attacks also cause session exhaustion on network devices that rely on session forwarding, and result in network breakdowns.



Principles of ICMP Flood Attack Defense

- To defend against ICMP flood attacks, the firewall can set a sending rate threshold of ICMP packets. ICMP packets whose sending rate exceeds the threshold will be discarded by the firewall.
- The firewall can set a threshold to the rate of ICMP packets based on interfaces or destination IP addresses.



Contents

1. Firewall Attack Defense Technologies
2. Single-Packet Attack Defense
- 3. DDoS Mitigation**
 - Principles of DDoS Mitigation
 - Configuration of DDoS Mitigation
4. Anti-DDoS

Setting DDoS Mitigation Parameters

- Set related parameters before enabling DDoS mitigation.

- Enable traffic statistics collection on an interface.

```
[FW] interface interface GigabitEthernet0/0/1  
[FW-GigabitEthernet0/0/1] anti-ddos flow-statistic enable
```

- Configure the traffic detection and cleaning modes.

```
[FW] ddos-mode { detect-clean | detect-only }
```

- Configure the sampling ratio for DDoS traffic statistics.

```
[FW] anti-ddos statistic sampling-fraction sampling-fraction
```

- Configure delays for enabling and disabling DDoS mitigation.

```
[FW] anti-ddos defend-time start-delay start-delay end-delay end-delay
```

- Configure an alarm threshold of the traffic rate for triggering DDoS mitigation.

```
[FW] anti-ddos destination-ip alert-rate alert-rate
```

- Configure the aging time for source IP address monitoring entries.

```
[FW] anti-ddos source-ip detect aging-time time
```

Configuration of DDoS Mitigation (1/2)

- Configure global SYN flood attack defense.

```
[FW] anti-ddos syn-flood source-detect
```

- Configure global HTTP flood attack defense.

```
[FW] anti-ddos http-flood source-detect [ mode { basic | advanced | redirect } ]  
[FW] anti-ddos http-flood defend alert-rate alert-rate
```

- Configure global HTTPS flood attack defense.

```
[FW] anti-ddos https-flood source-detect [ alert-rate alert-rate ]
```

- Configure global DNS request flood attack defense.

```
[FW] anti-ddos dns-request-flood source-detect mode { basic | auth-ns } [ alert-rate alert-rate ]
```

- Configure global DNS reply flood attack defense.

```
[FW] anti-ddos dns-reply-flood source-detect [ alert-rate alert-rate ]
```

- Configure global SIP flood attack defense.

```
[FW] anti-ddos sip-flood source-detect [ alert-rate alert-rate ]
```

Configuration of DDoS Mitigation (2/2)

- Configure global UDP flood attack defense.

```
[FW] anti-ddos udp-flood dynamic-fingerprint-learn [ alert-speed alert-speed ]
```

- Configure global UDP fragment attack defense.

```
[FW] anti-ddos udp-frag-flood dynamic-fingerprint-learn [ alert-speed alert-speed ]
```

- Configure ICMP flood attack defense.

- Configure interface-based DDoS mitigation.

```
[FW] interface interface GigabitEthernet0/0/1
```

```
[FW-GigabitEthernet0/0/1] anti-ddos icmp-flood [ alert-rate alert-rate ]
```

- Configure destination IP address-based rate limiting.

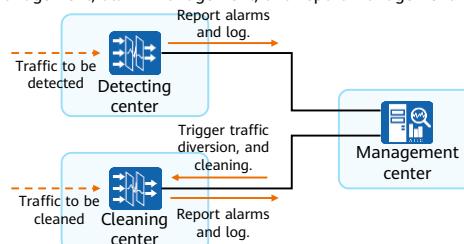
```
[FW] bandwidth-limit destination-ip type icmp max-speed max-speed
```

Contents

1. Firewall Attack Defense Technologies
2. Single-Packet Attack Defense
3. DDoS Mitigation
- 4. Anti-DDoS**
 - Anti-DDoS Solution Overview
 - Anti-DDoS Networking
 - Principles of Anti-DDoS
 - Configuration of Anti-DDoS

Anti-DDoS Solution Overview

- The anti-DDoS solution comprises the Anti-DDoS system and management center developed by Huawei. The anti-DDoS system comprises the detecting center and cleaning center. Therefore, the solution has a detecting center, cleaning center, and management center (SecoManager).
 - The detecting center detects traffic and reports exceptions to the management center. The management center then delivers traffic diversion policies to the cleaning center for traffic diversion and cleaning.
 - The cleaning center diverts and cleans traffic based on the policies delivered by the management center and re-injects the cleaned traffic. In this process, the cleaning center also logs the events and reports them to the management center.
 - The management center is in charge of centralized management of the detecting and cleaning centers. It is the core of the anti-DDoS solution. The management center provides diversified management functions, including device management, policy management, performance management, alarm management, and report management.



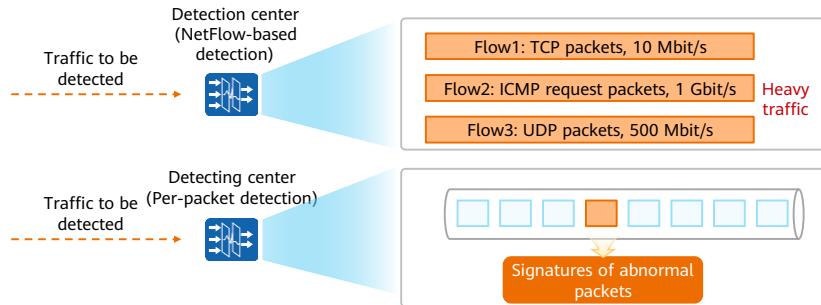
63 Huawei Confidential

 HUAWEI

- The Abnormal Traffic Inspection & Control System (ATIC) is a functional module of the SecoManager.

Detecting Center

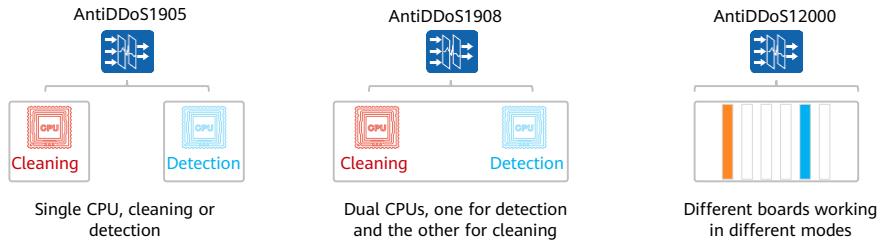
- The detecting technologies are NetFlow-based traffic detection and application-based packet detection technologies. The former detects only volumetric attacks, whereas the latter can further detect low-bandwidth attacks as well as application-layer DDoS attacks (such as SQL injection).
- The NetFlow-based traffic detection technology is only applicable to volumetric attack detection, due to the relatively large sampling ratio and NetFlow protocol restrictions. Most backbone networks and MANs have NetFlow devices deployed. Therefore, association with NetFlow devices is relatively low in the cost and applicable to volume-based attack detection on MANs or backbone networks.



- You can deploy traffic distribution devices (for optical fiber transmission) on networks or use flow mirroring to copy traffic to the traffic probe or detecting center.

Cleaning Center

- The cleaning center diverts and cleans traffic based on the policies delivered by the management center and re-injects the cleaned traffic. In this process, the cleaning center also logs the events and reports them to the management center. The cleaning center provides diversified DDoS traffic cleaning methods. It can accurately identify normal traffic and clean various types of abnormal traffic, including volume-based attacks, application-layer attacks, scanning and snooping attacks, and malformed packet attacks.
- A single-CPU fixed anti-DDoS device can only serve as the detecting device or cleaning device. A dual-CPU model can serve as both the detecting device and cleaning device by configuring the CPU type. For a modular anti-DDoS device, you can specify a board to work in detecting or cleaning mode.



ATIC System Architecture

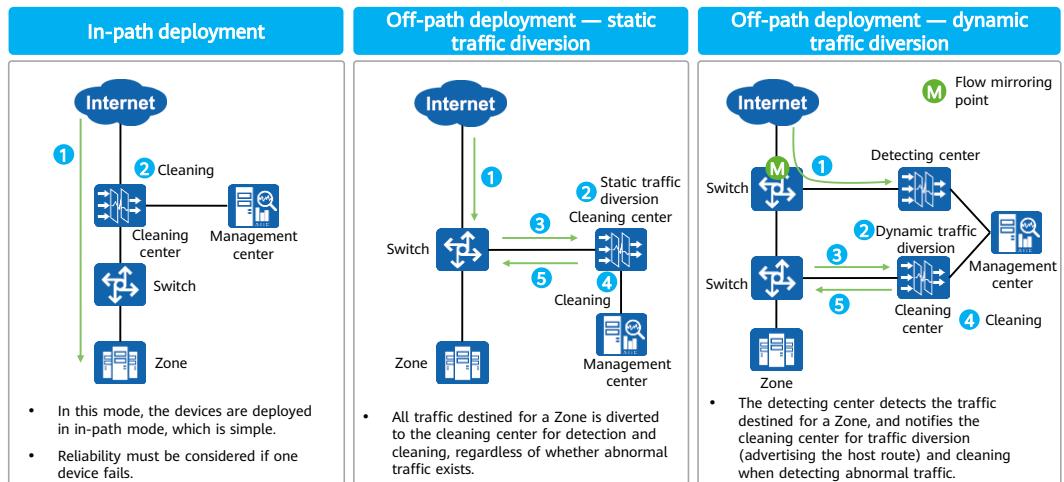
- SecoManager, as the management center (mainly its ATIC function module), uses the B/S architecture and is easy to deploy. You just need to install the software on an independent server to manage and monitor services. One management center can manage multiple geographically dispersed detecting and cleaning devices in a centralized manner.
- The ATIC consists of two components: management server and collector.
 - The ATIC management server manages detecting and cleaning devices, configures defense policies, and generates reports.
 - The ATIC collectors receive, summarize, and analyze attack logs sent from collectors and report them to the ATIC management server. They also store packet obtaining files for administrators to conduct further analysis.



Contents

1. Firewall Attack Defense Technologies
2. Single-Packet Attack Defense
3. DDoS Mitigation
- 4. Anti-DDoS**
 - Anti-DDoS Solution Overview
 - **Anti-DDoS Networking**
 - Principles of Anti-DDoS
 - Configuration of Anti-DDoS

Networking Modes of the Anti-DDoS Solution



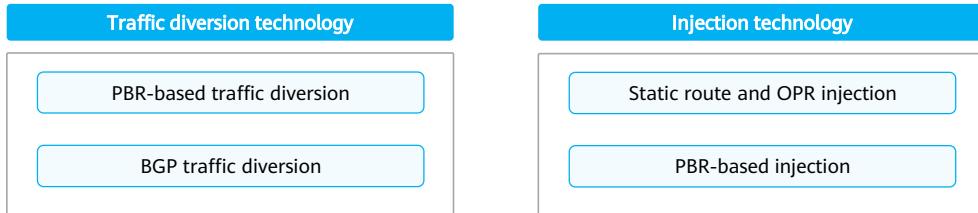
68 Huawei Confidential

HUAWEI

- In actual deployment, aside from copying traffic to the detecting center through flow mirroring, you can distribute traffic to the detecting center through deploying traffic distribution devices.

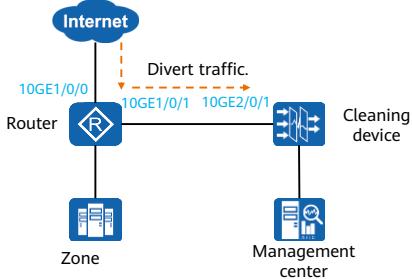
Traffic Diversion and Injection

- In an in-path deployment network, all service traffic needs to pass through the cleaning center. After being cleaned, the traffic is forwarded to a Zone based on the routing table.
- In an off-path deployment network, traffic does not pass through the cleaning center by default. You need to configure the traffic diversion and injection functions to implement traffic cleaning.
 - Traffic diversion: Network devices (such as routers and switches) send traffic destined for a Zone to the cleaning center.
 - Injection: The cleaning center sends cleaned traffic back to the network devices.
- Common traffic diversion and injection methods are as follows. They can be flexibly combined to implement traffic cleaning.



PBR-based Traffic Diversion

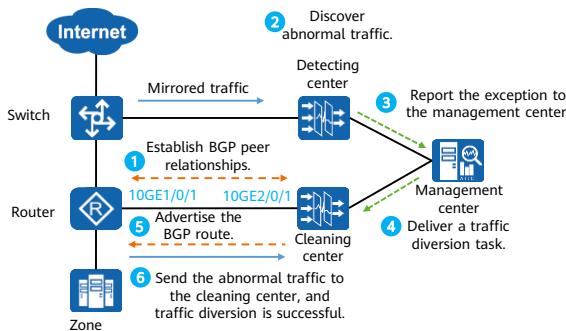
- PBR-based traffic diversion indicates configuring policy-based routing (PBR) on a core switch/router (connected to the cleaning device in off-path mode) to divert the traffic meeting conditions to the cleaning device. PBR needs to be configured only on the traffic diversion router, not on the cleaning device.
- PBR is usually used for static traffic diversion. In this mode, the inbound interface of the traffic to be diverted is specified. After the cleaning device cleans the traffic, the traffic is sent back to the diversion device, and is forwarded according to the routing table to avoid routing loops.



- Establish a traffic-diversion channel between 10GE1/0/1 of the router and 10GE2/0/1 (cleaning interface) of the cleaning device.
- Apply PBR on inbound interface 10GE1/0/0 of the router. In this way, the packets meeting conditions are forwarded to the cleaning device through 10GE1/0/1, rather than being forwarded according to the routing table. Therefore, traffic destined for a specified Zone is forcibly diverted.

BGP Traffic Diversion

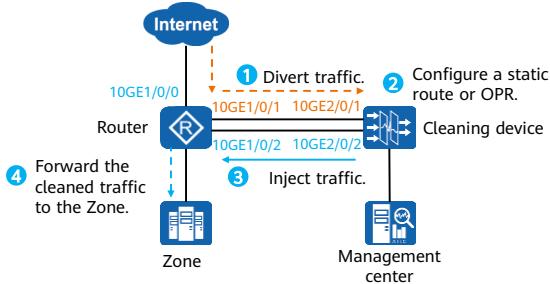
- BGP traffic diversion is a common dynamic traffic diversion mode. You need to configure BGP on the router and cleaning device in advance to establish BGP peer relationships. When detecting an exception, the management center delivers a traffic diversion task to the cleaning device. The cleaning device generates a 32-bit open programming route (OPR) and advertises the route to the router through BGP. The router searches for the BGP route in its routing table. Finally, the traffic originally destined for the Zone is sent to the cleaning center.



1. The router and the cleaning center establish BGP peer relationships through interconnection lines in advance.
2. The detecting center detects that the mirrored traffic is abnormal.
3. The detecting center reports the exception to the management center.
4. The management center delivers a traffic diversion task to the cleaning center.
5. The cleaning center generates a 32-bit OPR and advertises it to the router through BGP.
6. The router learns the BGP route and forwards the abnormal traffic to the cleaning center based on the routing table for traffic diversion.

Static Route and OPR Injection

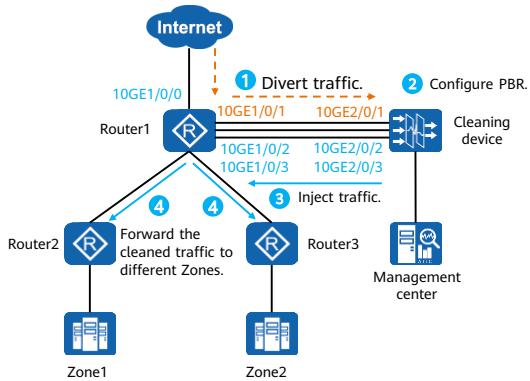
- You can configure static routes or OPRs on the cleaning device to inject cleaned traffic to network devices (such as routers and switches). The network devices send the cleaned traffic to the Zone based on their forwarding mechanisms.



1. The router uses a traffic diversion technology (PBR or BGP) to divert the traffic to be cleaned to the cleaning device.
2. Configure a static route or OPR pointing to the traffic-injection channel on the cleaning device.
3. The cleaning device cleans the traffic and sends the cleaned traffic to the network device through the traffic-injection channel.
4. The network device forwards the cleaned traffic to the Zone for traffic injection.

PBR-based Injection

- You can configure PBR on the cleaning device to inject cleaned traffic to different paths. Finally, the network device forwards the traffic to the Zone.

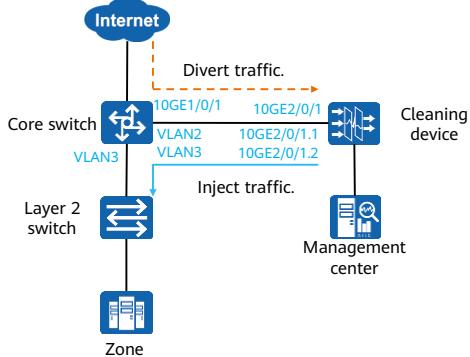


1. Router1 is a traffic-diversion router. A traffic-diversion channel is established between 10GE1/0/1 of Router1 and 10GE2/0/1 of the cleaning device. Traffic-injection channels are established between the other two interfaces of Router1 and the other two interfaces of the cleaning device.
2. Apply PBR on the inbound interface 10GE2/0/1 of the cleaning device.
3. The cleaning device injects traffic from different Zones to different interfaces (10GE1/0/2 and 10GE1/0/3) of Router1 based on PBR.
4. After the injected traffic reaches Router1, Router1 forwards the traffic to Router2 or Router3 based on its forwarding mechanism. Finally, the traffic reaches different Zones.

- During traffic injection, if BGP traffic diversion is used, apply PBR to 10GE1/0/2 and 10GE1/0/3 on Router1 to avoid routing loops. In this way, injected traffic will not be sent to the cleaning device.

Traffic Diversion and Injection in Layer 2 Networking Scenarios

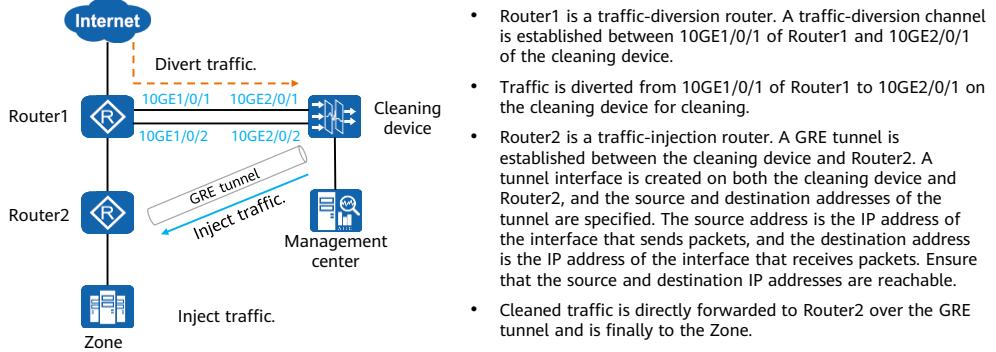
- If only a Layer 2 forwarding device rather than a Layer 3 forwarding device is deployed between the core switch and Zone, VLAN assignment can be used for traffic diversion and injection.



- The 10GE1/0/1 interface of the core switch is directly connected to the 10GE2/0/1 interface of the cleaning device. Create two VLANs on the switch, for example, VLAN2 and VLAN3.
- Two sub-interfaces 10GE2/0/1.1 and 10GE2/0/1.2 of the cleaning device are associated with VLAN2 (for traffic diversion) and VLAN3 (for traffic injection), respectively.
- The core switch diverts the traffic to the cleaning device through VLAN2 for cleaning. After cleaning, the cleaning device injects the cleaned traffic to the Zone through VLAN3.

Traffic Diversion and Injection in GRE Tunnel Scenarios

- When BGP is used for traffic diversion, injected traffic can be directly sent to the traffic-injection router (Router2 in the following figure) through a GRE tunnel and finally forwarded to the Zone to avoid loops.

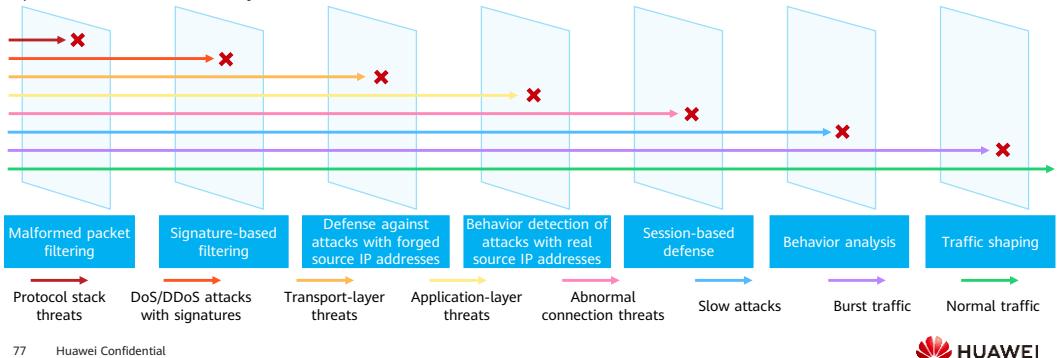


Contents

1. Firewall Attack Defense Technologies
2. Single-Packet Attack Defense
3. DDoS Mitigation
- 4. Anti-DDoS**
 - Anti-DDoS Solution Overview
 - Anti-DDoS Networking
 - Principles of Anti-DDoS**
 - Configuration of Anti-DDoS

Multi-Layer Traffic Detection Mechanism in Anti-DDoS Cleaning Center

- Huawei anti-DDoS devices deeply analyze each byte of every packet and use a seven-layer protection architecture, including malformed packet filtering, signature filtering, defense against attacks with forged source IP addresses, behavior detection of attacks with real source IP addresses, session-based defense, behavior analysis, and traffic shaping. Therefore, the devices can effectively identify multiple attack types, such as volume-based attacks, application attacks, scanning and sniffing attacks, and malformed packet attacks, and accurately clean DoS/DDoS attack traffic.



77 Huawei Confidential

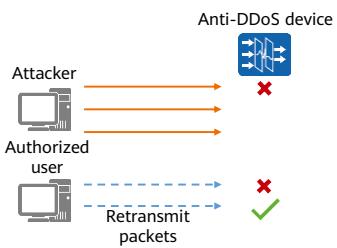
 HUAWEI

- Step 1 Malformed packet filtering: filters malformed packets that exploit protocol stack vulnerabilities and special control packets.
- Step 2 Signature-based filtering: filters attacks based on static packet signatures to defend against connectionless attacks, such as UDP flood, UDP reflection attacks (including DNS reflection attacks and NTP reflection attacks), and ICMP flood. Then static filtering based on the blacklist and whitelist is performed.
- Step 3 Defense against attacks with forged source IP addresses: defends against SYN flood attacks with forged source IP addresses.
- Step 4 Behavior detection of attacks with real source IP addresses: defends against DNS Query flood, DNS Reply flood, HTTP GET flood, HTTP POST flood, HTTPS flood, and SIP flood attacks launched from forged source IP addresses or botnets.
- Step 5 Session-based defense: defends against ACK flood, FIN flood, RST flood, TCP connection exhaustion, abnormal TCP session (sockstress, retransmission, null connection), DNS cache poisoning, SSL-DoS, SSL-DDoS, HTTP Slow headers, and HTTP Slow Post attacks.

- Step 6 Behavior analysis: traffic of attacks initiated by botnets greatly differs from that of user access. User access traffic is bursty, and access resources are scattered. As botnet attacks are launched by zombie tools, their attack traffic features constant access frequency and fixed access resources. Based on behavior analysis, CC attacks, TCP slow attacks, and TCP flood attacks with real source IP addresses can be defended against.
- Step 7 Traffic shaping: After layer-to-layer filtering, if the traffic is still heavy and exceeds the actual bandwidth of the server, intelligent rate limiting (based on source and destination IP addresses) is employed to ensure that the traffic reaching the server is within the secure bandwidth range of the server.

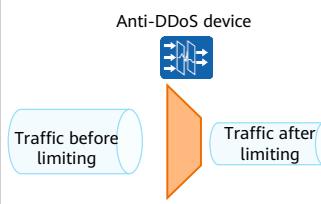
General Defense Mechanisms (1/2)

First-packet discarding



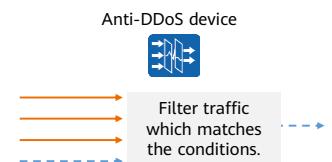
- For a data flow, the first received packet is not responded and is directly discarded. Normal service packets will be retransmitted, but a large number of random packets sent by attackers will not.

Rate limiting



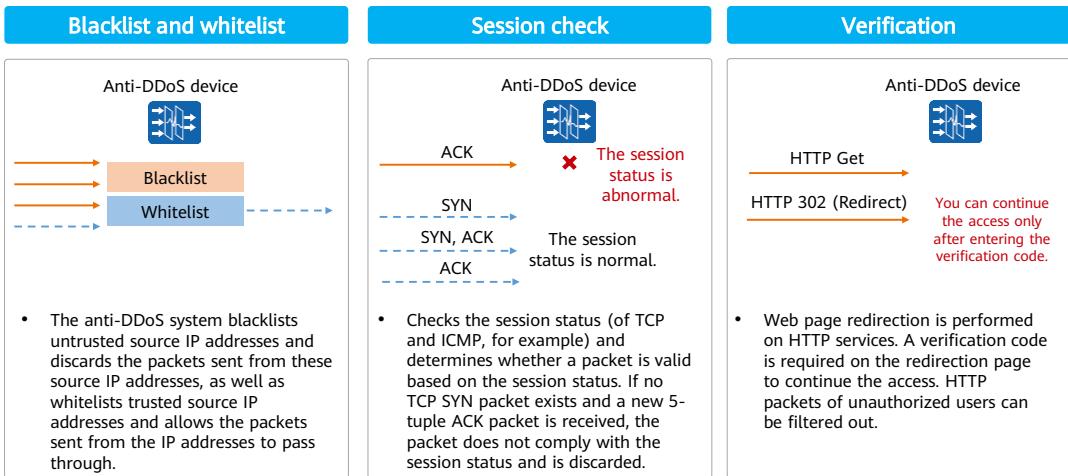
- You can limit the traffic volume or the number of connections for a data flow.

Filter



- A set of filtering conditions, including packet source IP address, destination IP address, protocol, and TTL, can be configured on the anti-DDoS device. If subsequent packets match these conditions, they match the filter, and the anti-DDoS device takes the specified action for these packets.

General Defense Mechanisms (2/2)



Defense Function Overview

IP defense

- IP flood traffic limiting
- IP flood defense

TCP defense

- TCP malformed packet defense
- SYN flood defense
- SYN-ACK flood defense
- ACK flood defense
- FIN/RST flood defense
- TCP connection flood defense
- TCP rate limiting

UDP defense

- UDP malformed packet defense
- UDP flood defense
- UDP traffic limiting

ICMP defense

- ICMP rate limiting

DNS defense

- DNS malformed packet defense
- DNS query flood defense
- DNS reply flood defense
- DNS rate limiting

SIP defense

- SIP flood defense
- SIP rate limiting

HTTP defense

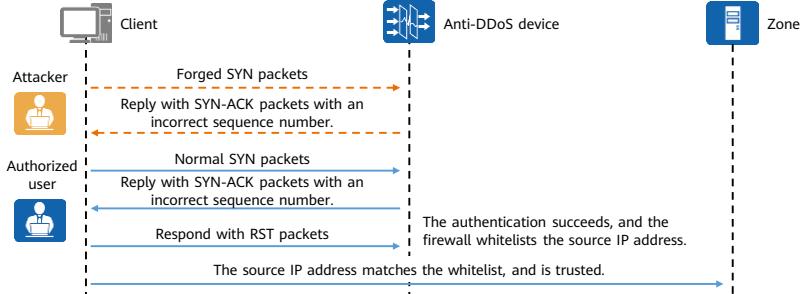
- HTTP flood defense
- Abnormal HTTP connection defense

HTTPS defense

- TLS encryption attack defense
- TLS session attack defense

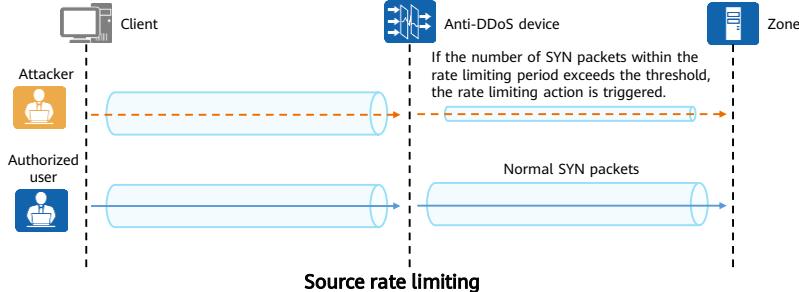
TCP Defense Mechanism - SYN Flood (1/2)

- Source authentication: After receiving a SYN packet, the anti-DDoS device sends a SYN-ACK packet back to the source IP address of the SYN packet. The anti-DDoS device determines the legitimacy of the source IP address by checking whether a response packet from the source IP address is received, preventing attacks with forged source IP addresses.
 - If the source IP address is forged, the client does not respond to the incorrect SYN-ACK packets. As a result, the authentication fails, and the anti-DDoS device discards subsequent SYN packets sent from this source IP address.
 - If the source IP address is real, the client responds with RST packets. As a result, the authentication succeeds, and the anti-DDoS device whitelists the source IP address and permits subsequent SYN packets.



TCP Defense Mechanism - SYN Flood (2/2)

- Source IP address monitoring: After source IP addresses are whitelisted, these real source IP addresses are still analyzed. Rate limiting is implemented on packets from abnormal source IP addresses to prevent attacks with real source IP addresses.
 - Source rate limiting: If the number of SYN packets within the rate limiting period exceeds the threshold, the rate limiting action is triggered.
 - Abnormal source blocking: If the number of anomalies exceeds the threshold within the consecutive detection period, the source IP address is added to the dynamic blacklist.

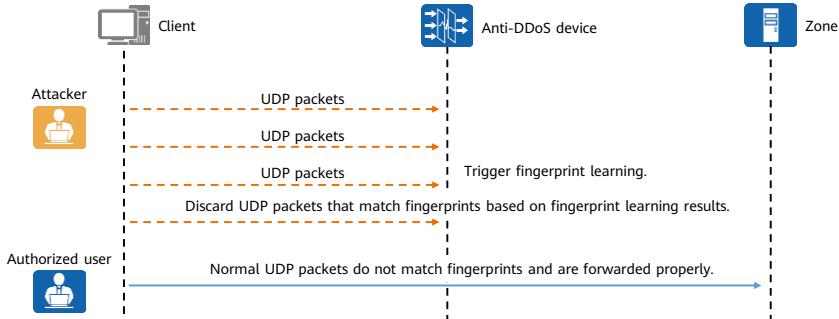


- Abnormal source IP blocking:

- Statistics on the ratio of SYN packets to ACK and SYN packets from the source address are collected, and the statistics are used to determine anomalies in a detection period.
- If the number of SYN packets in the detection period exceeds the threshold, an anomaly occurs.
- If the number of anomalies exceeds the threshold within the consecutive detection period, the source IP address is added to the dynamic blacklist.

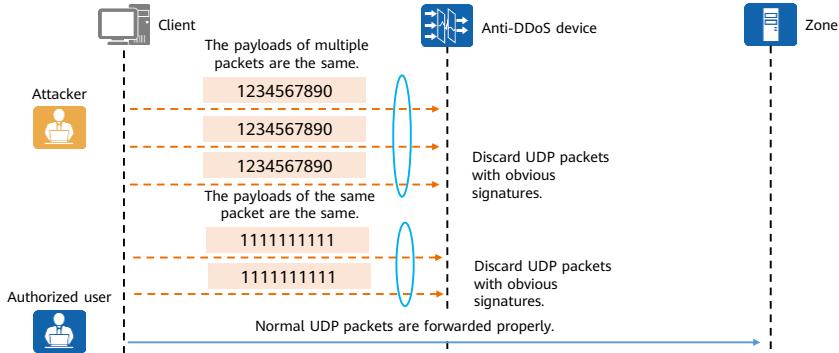
UDP Defense Mechanism - UDP Flood (1/3)

- Fingerprint learning: When UDP traffic exceeds the specific threshold, the fingerprint learning is triggered. The Anti-DDoS device dynamically generates fingerprints based on the signatures of attack packets and then discards any packets that match the fingerprints.



UDP Defense Mechanism - UDP Flood (2/3)

- Payload check: When the UDP traffic exceeds the threshold, the payload check is triggered. If the data segments of UDP packets are the same, the UDP packets are discarded as attack packets.



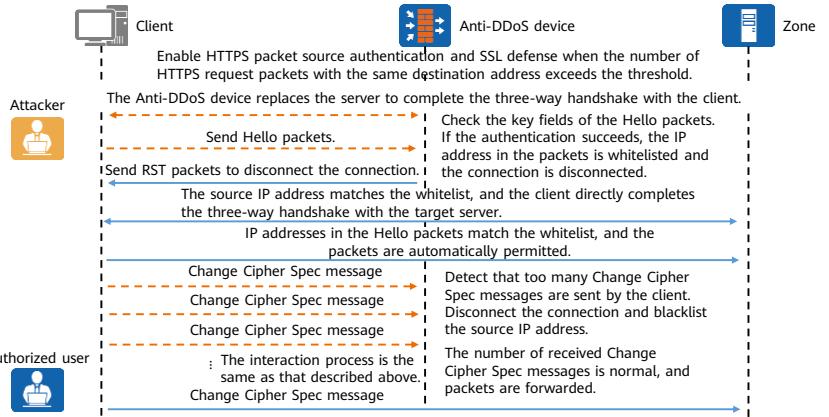
UDP Defense Mechanism - UDP Flood (3/3)

- Other defense mechanisms:
 - Session behavior detection: Malicious traffic is intercepted based on session check. If the interval for sending subsequent packets exceeds the preset threshold, interception is triggered.
 - Associated defense: The anti-DDoS device checks whether previous packets and subsequent packets in UDP sessions meet the matching rules.
 - If the UDP packet does not match the rule, the UDP packet is discarded.
 - If the UDP packet matches the rule, the source IP address of the UDP packet is whitelisted.
 - Rules to be matched by previous packets: destination IP address, protocol, destination port, packet length, and payload.
 - Rules to be matched by subsequent packets: destination IP address, destination port, packet length, and payload.
 - Watermark: The anti-DDoS device checks the watermark field carried in the packets and discards the packets that do not comply with the watermark requirement.
 - Parameters of the watermark algorithm: keyword 1, keyword 2, and destination port.

- Associated defense must be used together with session detection, and the interval for subsequent packets is set to 1 to 2 seconds. This function is enabled for independent game Zones.

HTTPS Defense Mechanism - SSL

- The anti-DDoS device collects statistics on the rate of HTTPS request packets by destination address and enables source authentication and SSL defense when the rate of HTTPS request packets exceeds the specified threshold.

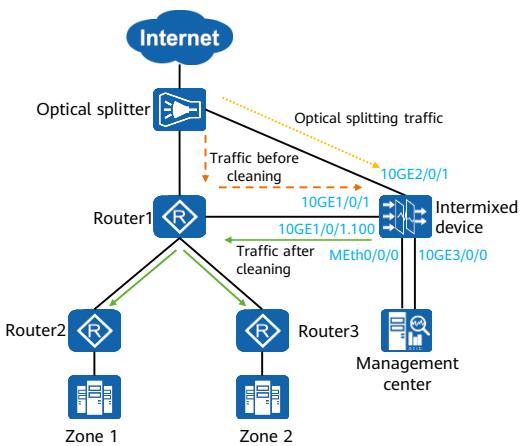


Contents

1. Firewall Attack Defense Technologies
2. Single-Packet Attack Defense
3. DDoS Mitigation
- 4. Anti-DDoS**
 - Anti-DDoS Solution Overview
 - Anti-DDoS Networking
 - Principles of Anti-DDoS
 - Configuration of Anti-DDoS**

Deploying AntiDDoS1900 (Intermixed Device) in Off-Path Mode

- Requirement description:
 - The intermixed device is deployed on the network node in off-path mode to detect and clean downstream traffic destined for the Zone. It copies traffic on the link to the detecting interface in optical splitting mode to detect traffic in real time, and notifies the management center upon anomalies. The management center delivers a traffic-diversion task to the cleaning SPU, so that traffic is diverted to the cleaning interface. Then, normal traffic is injected to the original link for further forwarding through the traffic-injection interface.
 - 10GE2/0/1 on the anti-DDoS device is used for receiving optical splitting traffic. Traffic passing through the interface is sent to the detecting SPU for analysis. 10GE1/0/1 is used for receiving diverted traffic. The cleaning SPU cleans the received traffic. Then, traffic is injected to the router for forwarding through subinterface 10GE1/0/1.100.



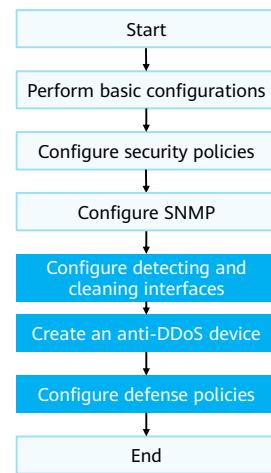
- Note: Only some anti-DDoS devices support the intermixed device.

Service Plan

Device	Interface	IP Address	Description
Intermixed device	10GE2/0/1	/	Detecting interface: It is used for receiving optical splitting traffic on the link and the IP address is not required.
	10GE1/0/1	10.1.2.1/24	Cleaning interface: It is an inbound interface for diverted traffic. The intermixed device applies diversified defense policies to the incoming traffic from the interface, and analyzes and cleans the traffic.
	10GE1/0/1.100	10.1.3.1/24	Injection interface: Traffic after cleaning is injected back to the original link through this interface.
	10GE3/0/0	10.1.5.1/24	Log interface used to communicate with the management center.
	MEth0/0/0	10.1.5.3/24	Management interface used to communicate with the management center.
Management center	/	10.1.5.2/24	IP address of the management center.

Configuration Roadmap

- Log in to the intermixed device and upgrade the software version.
- Load the license.
- Specify the CPU to implement detecting services.
- Create a user name, set a password, and configure STelnet.
- Set IP addresses for interfaces, add the interfaces to security zones, and enable interzone default packet filtering.
- Configure SNMP, so that the management center can obtain the status of the intermixed device.
- Configure detecting and cleaning interfaces and enable traffic statistics collection function on them.
- Log in to the management center, create an anti-DDoS device, and add a Zone.
- Configure proper defense policies.



- This example mainly describes how to configure the intermixed device and management center deployed on the network. Details on how to configure traffic diversion and injection, and defense policies are omitted.

Intermixed Device Configuration (1/2)

- Specify the CPU to implement detecting service and restart the service CPU for the setting to take effect.

```
<AntiDDoS1900> system-view  
[AntiDDoS1900] firewall ddos detect-spu slot 4 cpu 1  
[AntiDDoS1900] quit  
<AntiDDoS1900> save  
<AntiDDoS1900> reset cpu slot 4 1
```

- Configure SNMP.

```
[AntiDDoS1900] snmp-agent  
[AntiDDoS1900] snmp-agent sys-info version v3  
[AntiDDoS1900] snmp-agent mib-view included ddos iso  
[AntiDDoS1900] snmp-agent group v3 atic privacy read-view ddos write-view ddos notify-view ddos  
[AntiDDoS1900] snmp-agent group v3 atic privacy  
[AntiDDoS1900] snmp-agent usm-user v3 atic  
[AntiDDoS1900] snmp-agent usm-user v3 atic group atic  
[AntiDDoS1900] snmp-agent usm-user v3 atic authentication-mode sha2-512  
[AntiDDoS1900] snmp-agent usm-user v3 atic privacy-mode aes256  
[AntiDDoS1900] snmp-agent protocol source-interface MEth0/0/0
```

- Compared with SNMPv3, SNMPv2c is insecure. Therefore, SNMPv3 is recommended. This example uses SNMPv3 to describe the configuration procedure.

Intermixed Device Configuration (2/2)

- Configure the detecting interface.

```
[AntiDDoS1900] interface 10GE 2/0/1
[AntiDDoS1900-10GE2/0/1] anti-ddos detect enable
[AntiDDoS1900-10GE2/0/1] anti-ddos flow-statistic enable
[AntiDDoS1900-10GE2/0/1] quit
```

- Configure the cleaning interface.

```
[AntiDDoS1900] interface 10GE 1/0/1
[AntiDDoS1900-10GE1/0/1] anti-ddos clean enable
[AntiDDoS1900-10GE1/0/1] anti-ddos flow-statistic enable
[AntiDDoS1900-10GE1/0/1] quit
```

Management Center Configuration (1/3)

- Add an anti-DDoS device.
 - Choose **Device Management > Device > Device**. Click **Auto Discover** to add an anti-DDoS device and add SNMP and Stelnet parameters.

The screenshot shows the SecoManager Device Management interface. On the left, there's a sidebar for 'Security Device Group' with options like '+', 'Edit', and 'X'. Below it, a search bar for 'Enter device group name' and a dropdown menu showing 'All' and 'Ungrouped'. On the right, a main panel displays 'All logical devices: 2' (Normal: 2, Abnormal: 0). A dropdown menu under 'Add Device' has 'Auto Discover' selected, which is highlighted with a red box. The 'Auto Discover' dialog box contains fields for 'Management IP address' (with values '192.168.2.10' and '192.168.2.12') and a 'SNMPv3' configuration section. The 'SNMPv3' section includes fields for 'User name' (SHA2-512), 'Authentication protocol' (AES-256), 'Port' (161), 'Encryption algorithm' (AES-256), 'Encryption key' (8-255 characters), 'Retries (times)' (3), and 'Timeout period (ms)' (4000). At the bottom of the dialog are 'NETCONF' and 'STELNET' buttons. The overall interface is dark-themed with blue and white highlights.

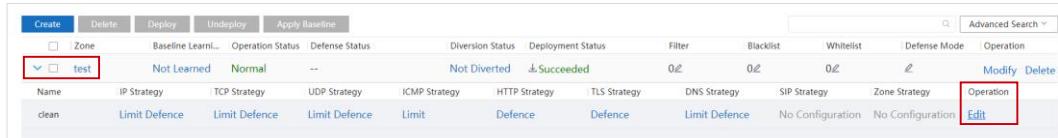
Management Center Configuration (2/3)

- A Zone is a device to be protected.
 - Choose **AntiDDoS Attack Defense** > **Attack Defense** > **Zone**. Click **Create** to add a Zone, associate device and add destination IP of the Zone.

The screenshot shows the SecoManager Management Center interface. On the left, there is a navigation bar with icons for Home, Create, Delete, Deploy, Undeploy, and Apply Baseline. Below this are tabs for Zone, Baseline Learning, and Operation Status. The main area displays a 'Create Zone' dialog box. This dialog includes fields for Name (set to 'User-defined' and 'Gaming'), Type (set to 'Automatic'), Industry (set to 'Gaming'), Associate device (empty), Description (empty), Traffic diversion mode (set to 'Automatic'), Defense mode (set to 'Automatic'), Blackhole mode (set to 'Automatic'), Second-Level blackhole (set to 'Automatic'), Dynamic blacklist mode (disabled), and Protection network / host (empty). There is also a 'Destination IP' section with a 'Create' button. At the bottom of the dialog are 'Cancel' and 'Confirm' buttons. The main interface below the dialog shows a table with 'Total records: 0' and a 'No data' message. The bottom right corner features the HUAWEI logo.

Management Center Configuration (3/3)

- After basic policies are configured, a basic attack defense policy is automatically generated on the devices associated with the Zone. You need to configure the attack defense policy based on live network traffic.
 - Choose **AntiDDoS Attack Defense** > **Attack Defense** > **Zone**. Click  of the corresponding Zone to display its configuration.
 - Click **Edit** in the **Operation** column to check the traffic baseline and defense policy information of the Zone and modify defense policies.
 - After a defense policy is configured, the configuration takes effect only after it is deployed on associated devices. Select the check box of a Zone and click **Deploy** to make the policy take effect.



Zone											Baseline Learni...	Operation Status	Defense Status	Diversion Status	Deployment Status	Filter	Blacklist	Whitelist	Defense Mode	Operation
  test	Not Learned	Normal	--	Not Diverted	 Succeeded	0/2	0/2	0/2												
Name	IP Strategy	TCP Strategy	UDP Strategy	ICMP Strategy	HTTP Strategy	TLS Strategy	DNS Strategy	SIP Strategy	Zone Strategy											
clean	Limit Defence	Limit Defence	Limit Defence	Limit	Defence	Defence	Limit Defence	No Configuration	No Configuration											

Quiz

1. (Single-answer question) Which of the following is not a malformed packet attack? ()
 - A. Teardrop attack
 - B. Smurf attack
 - C. LAND attack
 - D. Tracert attack
2. (True or false) Both the Ping of Death attack and ICMP flood attack are launched using ICMP packets. The difference is that Ping of Death attacks are launched by forging malformed ICMP packets while ICMP flood attacks are launched by DDoS. ()
 - A. True
 - B. False

1. D
2. A

Summary

- This course describes the attack defense technologies of firewalls, including the traditional single-packet attacks and DDoS attacks. Single-packet attacks include the scanning attack, malformed packet attack, and special packet attack. DDoS attacks include the SYN flood, HTTP flood, HTTPS flood, DNS request flood, DNS reply flood, SIP flood, UDP flood and ICMP flood attack.
- This course describes the anti-DDoS solution, networking modes, defense mechanisms, and configurations.
- After learning this course, you will be able to describe the principles of common cyber attacks and attack defense, and be familiar with related configurations.

Recommendations

- Huawei Official Websites
 - Enterprise service: <https://e.huawei.com/en/>
 - Technical support: <https://support.huawei.com/enterprise/en/index.html>
 - Online learning: <https://www.huawei.com/en/learning>

Acronyms and Abbreviations (1/2)

Acronym/Abbreviation	Full Name
ATIC	Abnormal Traffic Inspection & Control System
B/S	Browser/Server
BGP	Border Gateway Protocol
DDoS	Distributed Denial of Service
DNS	Domain Name Server
DoS	Denial of Service
GRE	Generic Routing Encapsulation
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol

Acronyms and Abbreviations (2/2)

Acronym/Abbreviation	Full Name
OPR	Open Programming Route
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSL	Secure Sockets Layer
SYN	Synchronous
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TTL	Time To Live
UDP	User Datagram Protocol

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。
Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

Copyright©2022 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product performance, market position, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.



Vulnerability Defense and Penetration Testing



Foreword

- In modern society, enterprise networks face various security threats, such as website attacks and database drag. Cyber security engineers need to know common cyber threats to properly defend against threats and prevent, identify, and block threats in a timely manner during O&M.
- Vulnerabilities are one of the main causes of security threats. This course uses vulnerabilities as an example to describe how to defend against security threats during security solution deployment and security O&M.

Objectives

- Upon completion of this course, you will be able to:
 - Describe the cyber kill chain.
 - Describe the harm of vulnerabilities.
 - Master vulnerability defense measures.
 - Explain the working principles of the intrusion prevention system.
 - Describe the penetration testing process.

Contents

1. Vulnerability

- Overview
 - Examples of Common Vulnerabilities

2. Vulnerability Defense

3. Penetration Testing

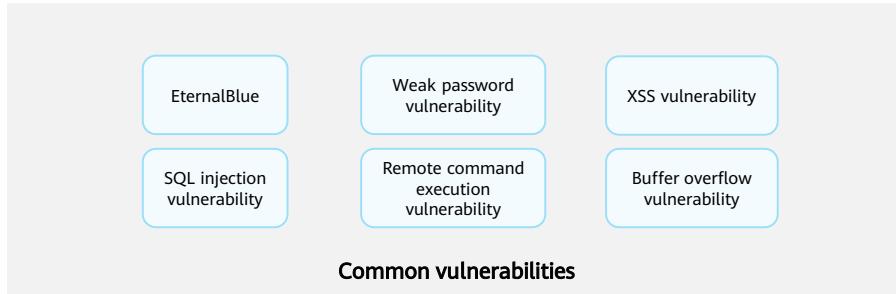
Cyber Kill Chain

- Lockheed Martin, a well-known enterprise, proposed the concept of "cyber kill chain", which divides the lifecycle of a cyber attack into seven stages.
- In the cyber kill chain, vulnerabilities are the entrance for attackers to intrude a network. If vulnerabilities exist on a network, the information system has security risks.

Reconnaissance	Weaponization	Delivery	Exploitation	Installation	Command and Control	Actions on Objectives
Research objectives and obtain objective information.	Couple exploit with backdoor into deliverable payload.	Deliver weaponized bundle to the victim via email, web, USB, etc.	Exploit vulnerability to execute code on a victim's system.	Install malware on the victim host to obtain the access permission.	Connect to and manipulate the victim host to obtain the persistent control permission.	Launch large-scale attacks, damage information systems, or steal data.

Overview

- In GB/T 25069-2022 Information security techniques — Terminology, vulnerabilities are defined as defects or improper configurations in software, hardware, or communication protocols of an information system that may be exploited by attackers to access or damage the system without authorization, resulting in security risks.
- A vulnerability is a weakness in a computer system, which threatens the confidentiality, integrity, availability, and access control of the system or its application data.



Vulnerability ID

- A vulnerability ID is released together with the vulnerability by a vendor to uniquely identify the vulnerability.
Vulnerabilities are recorded in the vulnerability databases of related organizations.
- Common Vulnerabilities and Exposures (CVE) is a list of publicly disclosed cyber security vulnerabilities. The CVE vulnerability ID is expressed as follows:
 - Each vulnerability is assigned a unique vulnerability ID in the format of CVE-year-/ID, for example, CVE-2019-0708.
 - Each CVE vulnerability contains the following information:
 - Description: brief description about the vulnerability source and modes of vulnerability-related attacks.
 - Reference: links to vulnerability-related reference information, such as vulnerability notices and suggestions provided by related vendors.
 - CNA: CVE Numbering Authority (CNA) that releases the vulnerability.
 - Release date: date when the vulnerability is released.

CVE-2019-0708 Detail	
The CVE Record information displayed on this page may not be displaying the full range of available information due to differences in how the data may have been entered. If you feel that the information being displayed is not meeting your expectations, please let us know by using this Feedback form .	
View full JSON 4.0 record	+
Description	A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Remote Desktop Services Remote Code Execution Vulnerability'.
State	PUBLIC
Problem Types	• Remote Code Execution
Vendors, Products & Versions	Vendor: Microsoft Product: Windows Versions Affected: <ul style="list-style-type: none">7 for 32-bit Systems Service Pack 17 for x64-based Systems Service Pack 1 Product: Windows Server Versions Affected: <ul style="list-style-type: none">2008 R2 for x64-based Systems Service Pack 1 (Core installation)2008 R2 for Itanium-Based Systems Service Pack 12008 R2 for x64-based Systems Service Pack 12008 for 32-bit Systems Service Pack 2 (Core installation)2008 for Itanium-Based Systems Service Pack 22008 for 32-bit Systems Service Pack 22008 for x64-based Systems Service Pack 22008 for x64-based Systems Service Pack 2 (Core installation)
References	• https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

6 Huawei Confidential



- CVE is released by CNAs. Currently, there are about 100 CNAs, including IT vendors, security companies, and security research organizations around the world. Any institution or individual can submit a vulnerability report to a CNA. Security vendor-type CNAs tend to encourage people to look for vulnerabilities, so they can enhance the security of their products.
- Not all vulnerabilities can be recorded in the CVE. A CNA determines whether to assign a CVE ID to a vulnerability based on the following rules:
 - The vulnerability can be fixed independently, and is not coupled with other vulnerabilities.
 - A software or hardware vendor acknowledges the existence of this vulnerability or releases an official notice.
 - The vulnerability affects only one code database. If a vulnerability affects multiple products, the vulnerability in each product is assigned an independent CVE ID.
- CVE vulnerability information is displayed on the website of the CVE program's organizer (<https://cve.mitre.org/>).
- Other public cyber security vulnerability databases:
 - National Vulnerability Database (NVD): the national vulnerability database for information security of the U.S. <https://nvd.nist.gov/>

Vulnerability Assessment

- The Common Vulnerability Scoring System (CVSS) is a widely used standard to score vulnerabilities.
- A CVSS score, ranging from 0.0 to 10.0, indicates vulnerability severity from least to most severe.

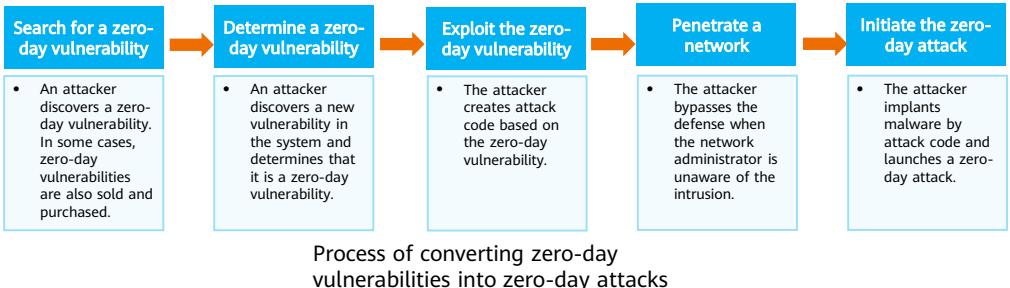
Level	Score
Critical	9.0-10.0
High	7.0-8.9
Medium	4.0-6.9
Low	0-3.9

- CVSS adopts a modular scoring system, which consists of three metric groups:
 - Base group: represents the intrinsic qualities of a vulnerability that are constant over time and across user environments. These are broken down into two main groups: Exploitability metrics, and Impact metrics.
 - Temporal group: reflects the characteristics of a vulnerability that change over time, such as the maturity of available exploitation code and the effort required for remediation.
 - Environmental group: looks at the characteristics of a vulnerability that are unique to a user's environment.

- CVSS is maintained by the Forum of Incident Response and Security Teams (FIRST), and the scoring criteria are published in <https://www.first.org/cvss/>.
- Relationship between CVE and CVSS:
 - A CVE is merely a dictionary of vulnerabilities. A CVE list does not contain CVSS scores. To view CVSS scores, use another vulnerability management system (for example, <https://www.cvedetails.com/>).
 - IT personnel prioritize vulnerabilities to be fixed based on CVE information and CVSS.
- Vulnerability types:
 - Critical vulnerability: vulnerability that can be exploited to obtain the permission of a server, and causes severe information leakage with a large impact scope.
 - High-risk vulnerability: vulnerability that can be exploited only through user interaction, and causes sensitive information leakage with a comparatively large impact scope.
 - Medium-risk vulnerability: information leakage or logical vulnerability with a medium impact scope.
 - Low-risk vulnerability: information leakage or logical vulnerability with a small impact scope.

Zero-Day Vulnerability

- Zero-day vulnerability: Also known as the zero-day exploit, which usually refers to a vulnerability that does not have a corresponding patch.
- Zero-day attack: A cyber attack launched by exploiting zero-day vulnerabilities to the system or software applications.
- Targets of zero-day attacks:
 - High-value targets: financial, medical, government, or military institutions.
 - Targets with a large impact scope: browsers, operating systems, and common application software.



Process of converting zero-day vulnerabilities into zero-day attacks

- Zero-day vulnerability: "zero-day" refers to the number of days that the corresponding patch does not appear after the vulnerability is disclosed. Generally, a vulnerability is called a zero-day vulnerability on the day it is released, because the corresponding patch has not been released on that day. If no patch is released after N days, the vulnerability is called an N-day vulnerability. "zero-day" does not indicate that the vulnerability has just been discovered. Hackers may have discovered vulnerabilities a long time ago, but they do not disclose them. For the public, a vulnerability can be called a zero-day vulnerability only when it is disclosed. Therefore, a zero day vulnerability refers to a vulnerability that "unknown to software vendors and the public", but "known to hackers or vulnerability traders".

Attack Domains

- In the cyber security field, attack and defense are the two most common topics. Attack strength grows when defense capability diminishes, and vice versa. With the development of networks, new attack methods emerge one after another. In the industry, The Common Attack Pattern Enumeration and Classification (CAPEC) classifies attacks into the following six fields:

Software	Hardware	Communications	Supply chain	Social engineering	Physical security
Attack patterns within this category focus on software systems of the targets. Common types include buffer overflow, command injection, code injection, SQL injection, brute force cracking, and identity spoofing.	Attack patterns within this category focus on hardware systems of the targets. Common types include infrastructure manipulation, resource manipulation, hardware fault injection, malicious logic insertion, and functionality misuse.	Attack patterns within this category sniff, eavesdrop on, steal or tamper with communication traffic. Common types include sniffing, man-in-the-middle (MITM), identity spoofing, communication channel manipulation, and protocol manipulation.	Attack patterns within this category focus on disruption of the supply chain lifecycle by manipulating computer system hardware, software, or services. Common types include illegal implantation of malicious code and software integrity attacks.	Attack patterns within this category exploit human weaknesses, behavior characteristics, and psychological characteristics to launch attacks, such as phishing attacks and password cracking.	Attack patterns within this category directly attack physical facilities and devices, such as physical theft and bypassing physical security.

9 Huawei Confidential



- There are many vulnerability-based attacks. Common types are as follows:
 - >Password cracking: Attackers use common or weak passwords for attempting to log in to common applications. If the login is successful, they obtain server management permissions.
 - Overflow attacks: Attackers exploit vulnerabilities in operating systems or common software to initiate attacks. If attacks are successful, hosts may be remotely controlled and implanted with malicious software, and systems may break down or restart.
 - Permission escalation: Attackers obtain higher permissions of the systems for further attacks, such as sending funds transfer instructions.
 - Virus intrusion: Attackers implant viruses for extortion, control hosts, or spread viruses to affect other host systems.
 - System damage: The system availability is damaged. For example, the Microsoft MS14-064 vulnerability can be exploited to cause the blue screen of death (BSOD).
 - Denial of Service (DoS): System resources are exhausted so that the target host cannot provide services externally.
 - Data theft: Attackers obtain confidential information for ransom or resell the information.

Contents

1. Vulnerability

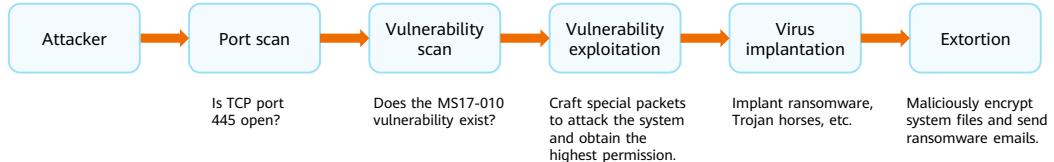
- Overview
- Examples of Common Vulnerabilities

2. Vulnerability Defense

3. Penetration Testing

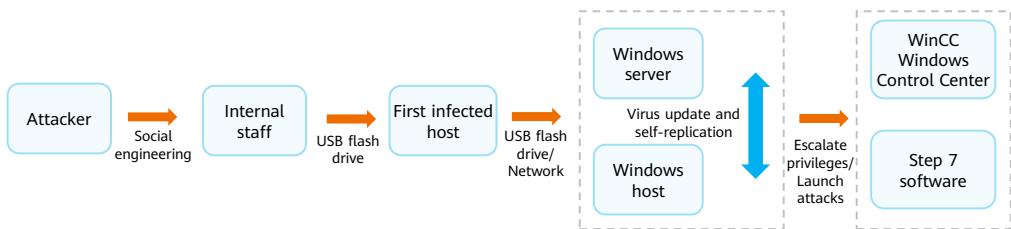
EternalBlue

- EternalBlue is a vulnerability of the Windows operating system. The vulnerability ID is MS17-010. It exploits the vulnerability of the SMB protocol in the Windows operating system to launch attacks and obtain the highest permission of the system. Then, malware such as ransomware, remote access Trojans (RATs), and cryptocurrency mining programs is implanted in the host.
- The attack process of EternalBlue is as follows:



Stuxnet

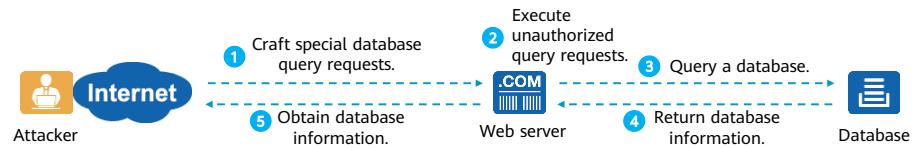
- Stuxnet is a virus that sweeps the global industry and the first worm that targets critical industrial infrastructure.
- Stuxnet features strong spreading capability, high concealment, and destructiveness. The attack process is as follows:



- If the software cannot be tampered with, the virus uses the 'win32k.sys' Keyboard Layout Privilege Escalation vulnerability (MS10-073) and Task Scheduler '.XML' Local Privilege Escalation vulnerability (MS10-092) to escalate the permission and tamper with Siemens control software again.
- After the control software is tampered with, the working frequency of the centrifuge reaches the threshold, resulting in overheating and scrapping.
- In this attack event, exploited MS10-046, MS10-061, MS10-073, and MS10-092 vulnerabilities are all zero-day vulnerabilities.

SQL Injection (1/2)

- In SQL injection, attackers exploit the vulnerability that web applications do not strictly filter user input data. The attackers construct special character strings as input to execute unauthorized malicious queries on the database server, leading to data leakage.
- The SQL injection process is as follows:



SQL Injection (2/2)

- The following is an example of obtaining the web application administrator's account through SQL injection:
 - An attacker enters the user name **' or 1=1 #** on the login page. It turns to the following SQL statement when being executed on the website:

```
select * from database.users where title like '%1'or 1=1 # %
```
 - The number sign (#) comments out the subsequent code. Therefore, the "where" condition changes to **title like '%1' or 1=1**, which is a condition of logical truth. In this case, all user names are returned.

User ID Submit

ID: 1' or 1=1 #	First name: admin	Surname: admin
ID: 1' or 1=1 #	First name: Gordon	Surname: Brown
ID: 1' or 1=1 #	First name: Hack	Surname: Me
ID: 1' or 1=1 #	First name: Pablo	Surname: Picasso
ID: 1' or 1=1 #	First name: Bob	Surname: Smith

- This slide shows only part of the process for obtaining the administrator's account and password through SQL injection.

Contents

1. Vulnerability
2. **Vulnerability Defense**
 - System Hardening and Patch Management
 - Intrusion Prevention
3. Penetration Testing

Linux System Hardening

- System hardening, also called host hardening, refers to implementing a series of security measures to improve the security of the operating system and reduce the risk of being attacked.
- The Linux operating system is hardened from the following aspects:

Account security settings	<ul style="list-style-type: none">• Lock or delete redundant accounts.• Set policies for passwords, such as password complexity.• Set the password expiration time.• Configure the function of locking an account after consecutive login failures.
System security settings	<ul style="list-style-type: none">• Set access control policies to restrict remote login.• Forbid remote login as a root user.• Change the automatic logout time of an account.• Change the listening port for remote login.
Service startup management	<ul style="list-style-type: none">• Disable unnecessary services.• Use iptables to set access rules.• Use services with the encryption function.
Log security settings	<ul style="list-style-type: none">• Configure user login logs.• Configure user operation logs.• Configure system security logs.

Windows System Hardening

- The Windows operating system is hardened from the following aspects:

Security configuration	<ul style="list-style-type: none">Cancel default sharingEnable the audit policy and record operation logs.Change the default TTL value to defend against probes or attacks.Disable unnecessary services.
Account security settings	<ul style="list-style-type: none">Restrict the number of users.Enable the account lockout policy.Enable the password policy.Deny remote access.
User permission settings	<ul style="list-style-type: none">Comply with the minimum authorization principle.Set different permissions for users of different levels.Periodically check account permissions.
Security center settings	<ul style="list-style-type: none">Virus and threat defenseFirewall and network protectionAccount protection, application and browser controlDevice security, performance, and running status

Patch Management

- Cyber security O&M engineers must upgrade patches in a timely manner as required to ensure system security.

General patch management

- You can refer to the fixing suggestions and patches for corresponding vendors provided by vulnerability databases (such as CVE, CNVD, and CNNVD) when vulnerabilities are released.

Linux patch management

- Linux is an open-source operating system. System patches are periodically released for different distributions (such as Red Hat, Ubuntu, and SUSE). You can update the system based on the patches released on the related official websites.

Windows patch management

- Microsoft releases patches for its operating systems and applications on the second Tuesday of each month, which is usually called the Patch Tuesday. In addition, Microsoft releases security bulletins to address key issues in operating systems and applications.

Application patch management

- Update and upgrade the applications based on the official patches.
- If necessary, you can update the software versions to improve security.

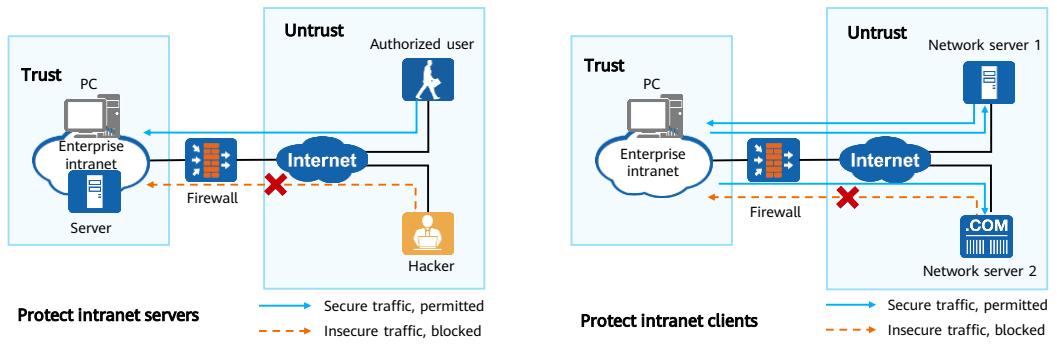
- Cyber security engineers can use terminal security tools to deliver patches or send emails to inform internal users to load patches.

Contents

1. Vulnerability
2. **Vulnerability Defense**
 - System Hardening and Patch Management
 - Intrusion Prevention
3. Penetration Testing

Overview of Intrusion Prevention

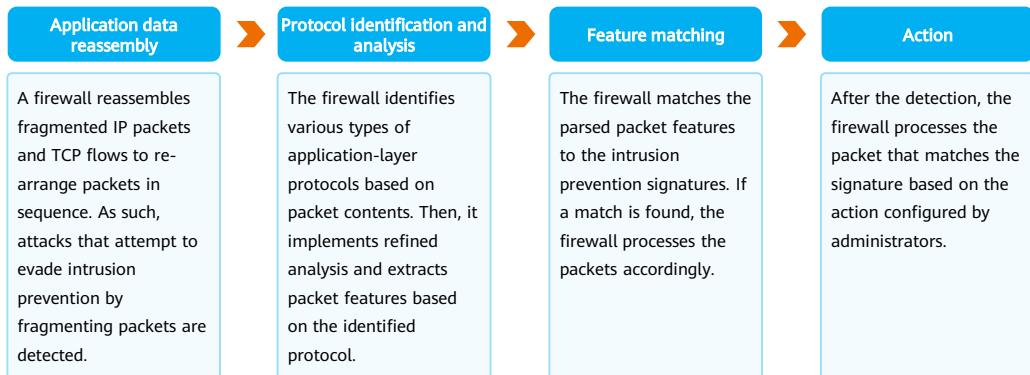
- Intrusion prevention is a security mechanism that detects intrusions (including buffer overflow attacks, Trojan horses, and worms) by analyzing network traffic, and terminates intrusion behaviors in real time using certain response methods, protecting enterprise information systems and network architectures from being attacked.
- The intrusion prevention function protects intranet servers and clients from internal and external intrusions.



- Intrusion prevention is a security prevention technology that can detect and prevent intrusion behaviors. After detecting network intrusions, the technology can automatically discard intrusion packets or block attack sources to fundamentally prevent attacks.
- Intrusion prevention has the following advantages:
 - Real-time attack blocking: A device is deployed on a network in in-line mode. When detecting intrusions, the device blocks intrusion and network attack traffic in real time, minimizing impacts of network intrusions.
 - In-depth protection: New attacks are hidden at the application layer of the TCP/IP protocol. Intrusion prevention can detect the contents of application-layer packets, reassemble network data flows for protocol analysis and detection, and determine the traffic that needs to be blocked based on the attack type and policy.
 - All-round protection: Intrusion prevention provides preventative measures against attacks, such as worms, viruses, Trojan horses, botnets, spyware, adware, Common Gateway Interface (CGI) attacks, cross-site scripting attacks, injection attacks, directory traversal attacks, information leakage, remote file inclusion attacks, overflow attacks, code execution, DoS attacks, and scanning tools. All-round protection comprehensively helps defend against various attacks and protect network security.
 - Internal and external prevention: Intrusion prevention protects enterprises from both external and internal attacks. The device detects traffic that passes through, protecting both servers and clients.
 - Precise protection: The device can update its intrusion prevention signature database periodically from the cloud-based security center so that it can detect new threats. This ensures effective intrusion prevention.

Intrusion Prevention Implementation

- The basic implementation mechanism of intrusion prevention is as follows:



Signature

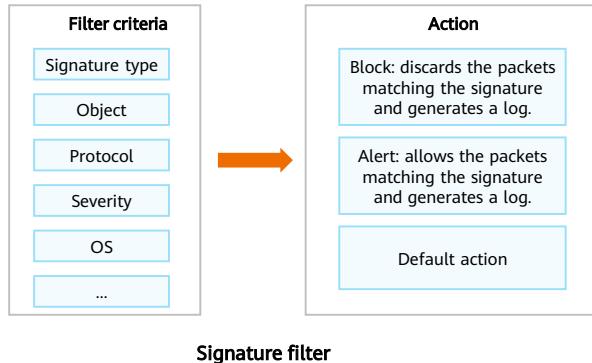
- Intrusion prevention signatures describe the features of network attacks. A firewall detects and defends against attacks by comparing data flows with the signatures.

Predefined signature	User-defined signature
<ul style="list-style-type: none">• Predefined signatures are those preset in the intrusion prevention system (IPS) signature database. They are fixed, that is, they cannot be created, modified, or deleted.• Each predefined signature has a default action. The details are as follows:<ul style="list-style-type: none">▫ Allow: Packets matching the signature are allowed to pass through and no log is recorded.▫ Alert: Packets matching the signature are allowed to pass through and logs are recorded.▫ Block: Packets matching the signature are denied and logs are recorded.	<ul style="list-style-type: none">• User-defined signatures refer to those created by administrators based on customized rules.• If new types of attacks emerge, their matching signatures are not available in the IPS signature database immediately. If users are familiar with the attacks, they can create user-defined signatures for defending against these attacks.• After user-defined signatures are created, the system automatically checks the validity of the corresponding user-defined rules to prevent inefficient signatures from wasting resources.• The actions for user-defined signatures can be Block or Alert. When creating user-defined signatures, administrators can configure actions as needed.

- You are advised to configure user-defined signatures only when you understand the attack features. Incorrect user-defined signatures may lead to invalid configurations, packets loss, or service interruptions.

Signature Filter

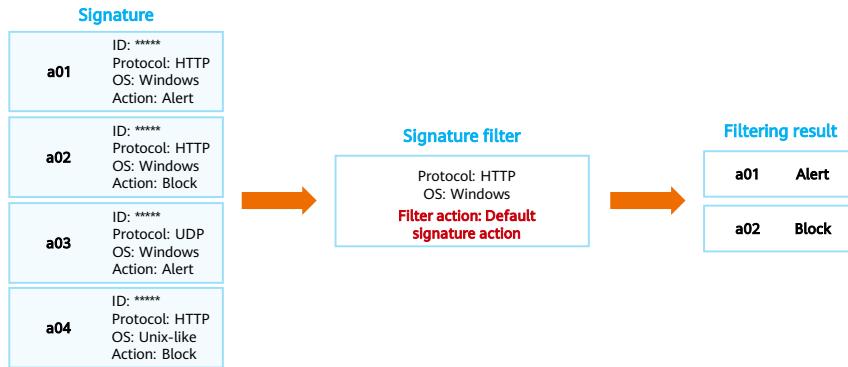
- An IPS signature database contains a large number of signatures for various attacks. However, in the actual network environment, not all signatures are required. In this case, you need to configure a signature filter. The IPS defends against only the filtered signatures.



- It is difficult to configure a signature filter because you must be familiar with networks and services. The IPS provides default IPS profiles for common scenarios.
- Note that multiple values can be configured for a filtering condition and these values are ORed.
- In most cases, the default actions for signatures are used for the filtered signatures in the signature filter. You can also set actions for all signatures in the filter. The action of a signature filter has a higher priority than the default action of a signature. If a signature filter does not use the default action of a signature, the action configured for the signature filter takes effect.
- Signature filters configured earlier have higher priorities. If two signature filters in one profile contain the same signature, packets matching the signature are processed according to the signature filter with a higher priority.
- When a packet matches multiple signatures, the actual action for the packet is as follows:
 - If the actions for all the matched signatures are **Alert**, the action for the packet is **Alert**.
 - If the action for any matched signature is **Block**, the action for the packet is **Block**.

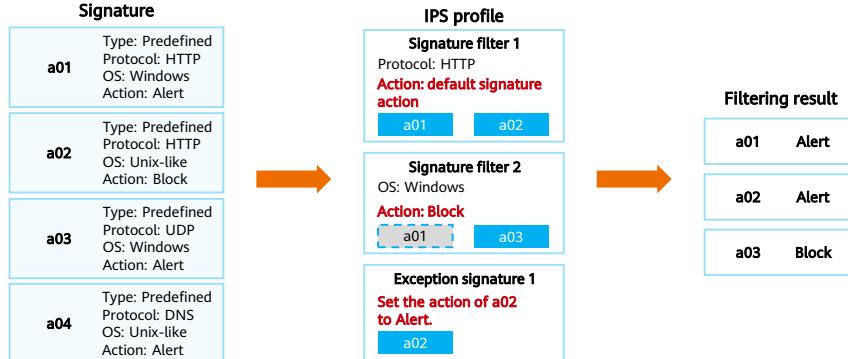
Signature Filter Example

- If the protected target is a web server running the Windows operating system, you can configure the signature filter to filter out the signatures whose operating system is Windows and protocol is HTTP.



Exception Signature

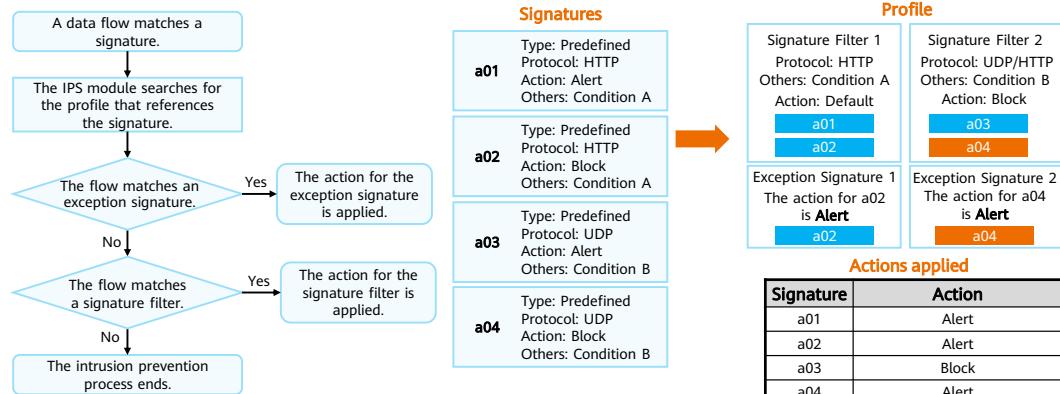
- A unified action is configured for signatures in a signature filter and you are not allowed to modify the action for a single signature. Considering requirements in some exceptions, the IPS provides the exception signature function. The action for an exception signature has a higher priority than that for a signature filter.



- The action set for an exception signature can be Block, Alert, Allow, or Blacklist. Blacklist means adding the source or destination address of related packets to the blacklist when traffic is blocked.
- In an IPS profile, multiple signature filters and exception signatures can be configured, which together determine the final response action for a signature. The action for an exception signature, action for a signature filter, and the default action for a signature are listed in descending order of priority.

Traffic Processing Flow

- If a data flow matches an intrusion prevention profile, a device sends the data flow to the intrusion prevention module and matches the data flow against the signatures referenced in the intrusion prevention profile in sequence.



27 Huawei Confidential



- When a data flow matches multiple signatures:
 - If the actions for these signatures are all **Alert**, the action applied to the data flow is **Alert**.
 - If the action for any signature is **Block**, the action applied to the data flow is **Block**.
- If the data flow matches multiple signature filters, the action for the signature filter with the highest priority is applied to the data flow.

Contents

1. Vulnerability
2. Vulnerability Defense
- 3. Penetration Testing**

Penetration Testing Overview

- **Concept:** Penetration testing engineers simulate attack technologies and vulnerability discovery technologies that may be used by hackers to perform in-depth detection on the security of target networks, hosts, and applications to find the most vulnerable parts of the system.
- **Purpose:** The purpose of penetration testing is defense. Security experts analyze the causes of vulnerabilities and provide rectification suggestions to defend against attacks from malicious attackers.
- **Classification:** white-box testing, black-box testing, and gray-box testing.

- According to the Cybersecurity Law of the People's Republic of China issued on June 1, 2017, the security test can be performed only after being authorized by the customer of the target system. It is illegal to perform the test without authorization.
- Penetration testing classification:
 - White-box testing: Penetrate a website when its source code, logical architecture, and other information are known. The process is similar to code analysis.
 - Black-box testing: Penetrate a website when only the website domain is known. Only the result is concerned.
 - Gray-box testing: a test mainly used in the integration test phase, focusing on not only the correctness of output and input, but also the internal logic of the program. Gray-box testing is not as detailed and complete as white-box testing, but focuses more on the internal logic of programs than black-box testing. Gray-box testing usually determines the internal running status of a programme based on representative phenomena, events, and flags.

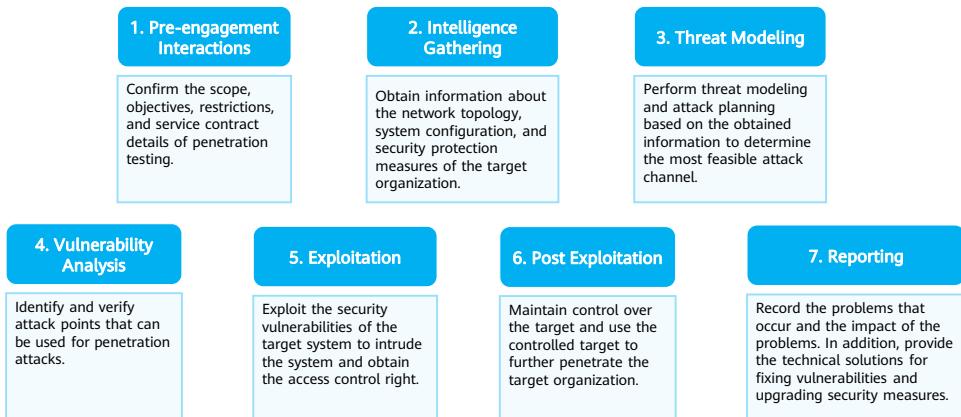
Penetration Testing Framework

- Penetration testing is a specific method for implementing security evaluation. Penetration testing methods vary greatly in industries and evaluation objects. After long-term exploration and demonstration, a series of security testing methods applicable to networks, applications, and systems gradually come into being in the industry. Some well-known security evaluation methodologies are listed below.

- Penetration Testing Execution Standard (PTES)
- Open Source Security Testing Methodology Manual (OSSTMM)
- Information Systems Security Assessment Framework (ISSAF)
- Open Web Application Security Project (OWASP)
- Web Application Security Consortium Threat Classification (WASC-TC)

Penetration Testing Process

- This slide describes the test process of the Penetration Testing Execution Standard (PTES).



Common Tools for Penetration Testing



- Wireshark: an open-source network protocol analyzer for multiple platforms. You can use it to browse obtained data in a timely manner and view packet details.
- Tcpdump: a packet obtaining and data packet analysis tool used for network sniffing.
- Nessus: a vulnerability scanning program applicable to the UNIX system.
- Snort: an open-source intrusion detection and prevention system. It can obtain, analyze, and record network traffic, and supports vulnerability scanning.
- Aircrack: a tool for cracking wireless network keys.
- John the Ripper: a quick password cracking program that can detect weak passwords in the system.
- Metasploit: an open-source vulnerability detection tool and a software framework for penetration testing.
- Kali Linux: a Linux distribution that provides a variety of security and forensics tools and a rich development environment.

Penetration Testing Tool - Wireshark

- As shown in the following figure, when a user logs in to a network device through Telnet, the user can use Wireshark to obtain packets and login passwords.



Penetration Testing Tool — Nmap

- Network Mapper (Nmap) is a network scanning and sniffing tool in Linux. It is now developed as a comprehensive cross-platform scanning software that supports multiple operating systems, such as Windows, Linux, and macOS.
- Nmap provides the following scanning functions:
 - Host discovery: checks whether the target host is online.
 - Port scan: detects port status and provided services.
 - Operating system detection: detects the operating system running on the host.



Quiz

1. (True or false) Unauthorized penetration testing is an attack. ()

- A. True
- B. False

1. A

Summary

- This course uses vulnerabilities as an example to describe common security threats on the network, vulnerability defense solutions such as system hardening, as well as penetration testing process and tools.
- Upon completion of this course, you will be able to understand common security threats on the network and defend against common security threats during security deployment and O&M.

Recommendations

- Huawei official websites:
 - Enterprise service: <https://e.huawei.com/en/>
 - Technical support: <https://support.huawei.com/enterprise/en/index.html>
 - Online learning: <https://www.huawei.com/en/learning/>

Acronyms and Abbreviations

Acronym/Abbreviation	Full Name
B/S	Browser/Server
C/S	Client/Server
CGI	Common Gateway Interface
CVE	Common Vulnerabilities and Exposures
DNS	Domain Name Server
OS	Operating System
SMB	Server Message Block
SQL	Structured Query Language
TCP	Transmission Control Protocol
TTL	Time to Live

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。
Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

Copyright©2022 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product performance, market position, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.



Content Security Filtering Technologies



Foreword

- With the development of the times, the society has entered the mobile Internet era. Security threats gradually extend to the application layer. More and more enterprises start to pay attention to the security of internal information, such as the leakage of core confidential information. Therefore, the administrator needs to identify risks in service scenarios based on service security requirements and take corresponding risk control measures. The content security filtering technology of Huawei firewalls helps enterprises manage and control content security.
- This course describes the concepts and implementation of content security filtering technologies on firewalls.

Objectives

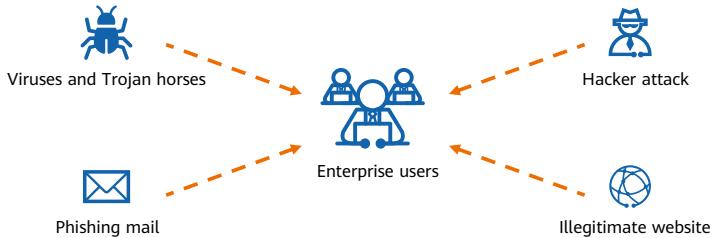
- On completion of this course, you will be able to:
 - Describe the technical background of the content security filtering technologies.
 - Describe basic principles of content security filtering technologies.
 - Master the configuration of content security filtering technologies.

Contents

- 1. Overview of Content Security Filtering Technologies**
2. Principles of Content Security Filtering Technologies
3. Examples for Configuring Content Security Filtering Technologies

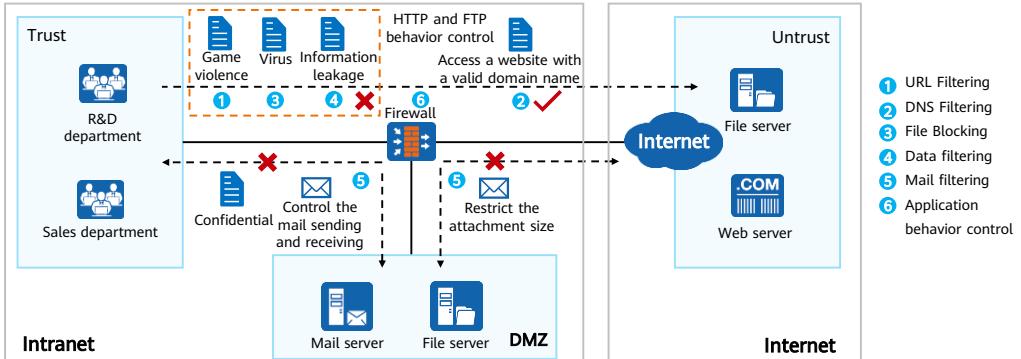
Technical Background of Content Security Filtering Technologies

- With the development of communications, security threats are evolving from simple cyber threats to application and data security threats. In addition, the requirements for internal service security of enterprises are increasing. It is a great challenge for enterprises to identify confidential information or illegitimate and low-quality information in service scenarios, generate alarms, and block such information.
- User behavior management and control is a powerful measure to solve the security problems enterprises are facing. Deploying content security filtering technologies on Huawei firewalls can help implement refined management and control on user behaviors.



Introduction to Content Security Filtering Technologies

- Content security filtering technologies deployed on Huawei firewalls can be applied to different security protection solutions based on scenario requirements. These technologies help enterprises manage and control content security while preventing core information leakage and adverse impacts caused by improper user behaviors.
- The content security filtering technology helps enterprises manage content security and prevent core information leakage.



5 Huawei Confidential

HUAWEI

- Content security filtering technologies can be used to control enterprise user behaviors. For example, users are not allowed to access illegitimate websites to prevent adverse impacts on enterprises as well as entertainment websites during working hours to improve work efficiency.
- Content security filtering:
 - URL filtering regulates online behaviors by controlling URLs that users can access, thereby permitting or rejecting users' access to specified web page resources.
 - DNS filtering is implemented in the domain name resolution phase to prevent employees from accessing illegitimate content or malicious websites, which may cause threats such as viruses, Trojan horses, and worms.
 - File blocking blocks the transmission of certain types of files, which reduces risks of executing malicious codes and viruses on the internal network and prevents employees from transmitting enterprises' confidential files to the Internet.
 - Data filtering falls into two types: file data filtering and application data filtering. File data filtering filters the uploaded and downloaded files by keyword. You can specify the protocols for file transfer or the types of files to be filtered. Application data filtering filters application content by keyword. The device filters different data for different applications.
 - Mail filtering: filters mails by checking the email addresses of the sender and recipient, attachment size, and number of attachments.
 - The application behavior control function is used to accurately control users' HTTP and FTP behaviors (such as upload and download).

Contents

1. Overview of Content Security Filtering Technologies
2. **Principles of Content Security Filtering Technologies**
 - URL Filtering
 - DNS Filtering
 - File Blocking
 - Data Filtering
 - Mail Filtering
 - Application Behavior Control
3. Examples for Configuring Content Security Filtering Technologies

Overview of URL Filtering

- The URL filtering function regulates online behaviors by controlling URLs that users can access, thereby permitting or rejecting users' access to specified web page resources. This function allows enterprises to allocate Internet bandwidth resources in a refined manner and accurate control employees' Internet access permissions.

Prohibiting Access to Irrelevant Websites

- The URL category and blacklist/whitelist functions allow users to access only specified URLs, improving office efficiency.

Blocking Low-Reputation and Malicious URLs

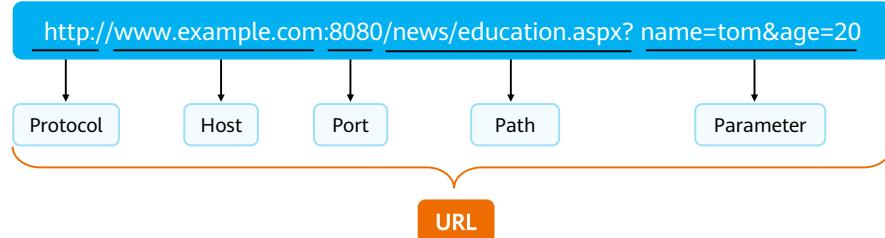
- Identifying low-reputation and malicious URLs can effectively block network attacks from malicious websites and enhance network security protection.

Controlling URL Access by Schedules

- Defining URL access policies for different schedules can implement schedule-based URL access control, thus effectively utilizing enterprise network bandwidth resources.

URL Structure

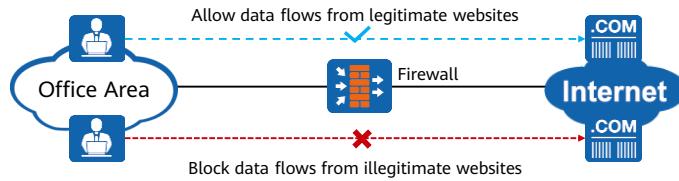
- Each web page on the Internet has a unique identifier, that is, the URL. A URL is a specific address assigned to each available resource on the network so that the resource can be located or identified. Therefore, each resource (page, site, document, file, folder) on the Internet has a URL.
- A URL consists of fields such as Protocol, Host, Path, and Parameter.



- The field meanings are as follows:
 - Protocol: scheme/protocol. It tells the browser how to handle the file to be opened. HTTP is most commonly used. Generally, this parameter is optional for HTTP.
 - Host: indicates the domain name or IP address of the web server. If the web server uses a non-standard port (not port 80, for example, 8080), the Host field also needs to contain the port number, for example, www.example.com:8080.
 - Path: indicates the directory or file name on the web server, separated by slashes (/).
 - Parameter: indicates the parameter transferred to the web page. This parameter is generally used for dynamic data query from the database.

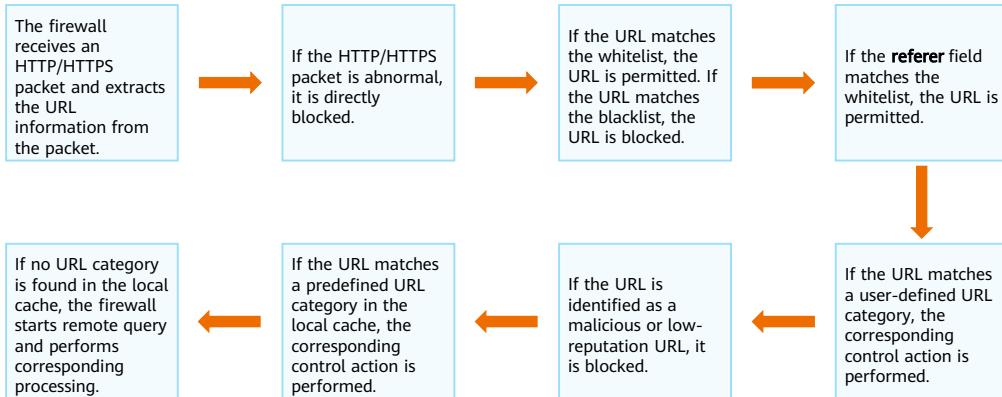
Principles of URL Filtering

- The basic principles of URL filtering are as follows:
 - A user uses a browser to initiate a website access request. The request packet reaches the firewall through the enterprise intranet.
 - The firewall parses the received HTTP/HTTPS request packet, obtains the URL information, and analyzes the URL information.
 - If the URL is legitimate, the HTTP request is passed and the user can browse the website.
 - If the URL is illegitimate, the HTTP request is blocked and an alarm page is pushed.



Process of URL Filtering

- If the URL filtering function is enabled on the firewall, the firewall performs URL filtering when a user accesses a network resource using HTTP or HTTPS through the firewall. The process is as follows:



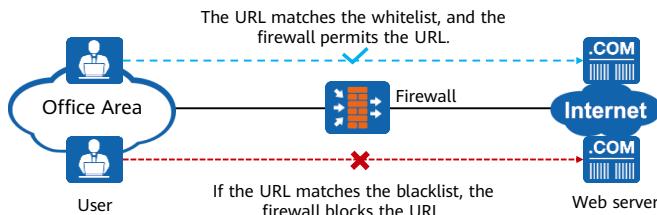
URL Filtering Mode

- When a user's URL access request matches a URL rule, the firewall processes the URL access request based on the URL filtering mode. URL filtering can be implemented in the following modes:

Blacklist and Whitelist	URL Categories	Low-Reputation or Malicious URL	External Dynamic Malicious URL
<ul style="list-style-type: none">The blacklist is a list of URLs inaccessible to users.The whitelist is a list of URLs accessible to users.The processing priority of the whitelist is higher than that of the blacklist.	<ul style="list-style-type: none">A large number of URLs are classified into different URL categories to control a certain type of websites.URL categories are classified into predefined categories and user-defined categories.User-defined URL categories take precedence over predefined URL categories.	<ul style="list-style-type: none">URL reputation reflects the reliability of the URL that a user accesses. After URL reputation detection is enabled, low-reputation URLs can be blocked.Malicious URLs refer to URLs containing malicious information. After malicious URL detection is enabled, malicious URLs can be blocked.	<ul style="list-style-type: none">The external dynamic malicious URL list is a text file of some malicious URLs released by external official websites. You can load the external dynamic malicious URL list to identify and block the latest malicious URLs, preventing users from new attacks.

URL Blacklist and Whitelist

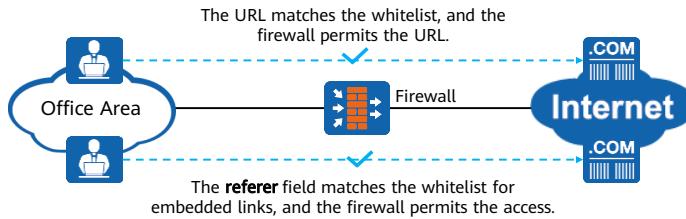
- The blacklist is a list of URLs inaccessible to users, and the whitelist is a list of URLs accessible to users. The blacklist and whitelist are generally used to filter simple and fixed websites.
- When a user requests to access a URL, the device matches the extracted URL information with the blacklist and whitelist. If the URL matches the whitelist, the URL is permitted. If the URL matches the blacklist, the URL is blocked.
- The blacklist and whitelist identify URLs at a finer granularity. Therefore, in URL filtering, the priority of the blacklist/whitelist-based filtering mode is higher than that of user-defined and predefined URL categories. The priority of the whitelist is higher than that of the blacklist.



- The blacklist and whitelist are generally used to filter simple and fixed websites. Compared with URL categories, the blacklist and whitelist have finer category granularities. When a user requests to access a URL, the device matches the extracted URL information with the blacklist and whitelist.
 - If the URL matches the whitelist, the URL request is permitted. For example, an enterprise allows employees to access only some work-related websites. To achieve this requirement, you can add some work-related websites to the whitelist.
 - If the URL matches the blacklist, the URL request is blocked. For example, to improve work efficiency of employees and fully utilize network bandwidth, enterprises need to control online behaviors of employees and prevent them from accessing entertainment, game, and video websites. To achieve this requirement, you can add entertainment, game, and video websites to the blacklist.

Whitelist for Embedded Links

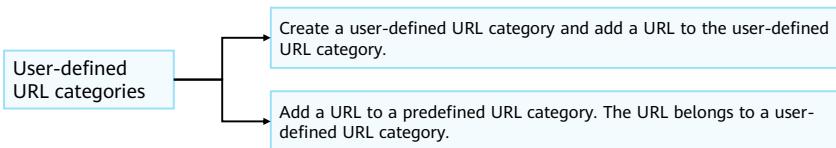
- Generally, large web pages are embedded with links to other web pages. If only the main web page is added to the whitelist, the embedded links to other web pages in the main web page cannot be accessed. To access the embedded links, all of them need to be whitelisted, which, however, involves complex configurations.
- To solve this problem, whitelist for embedded links is added. The system matches the **referer** field in a user's HTTP request with the whitelist for embedded links. If they are matched, the user can access the web page. Therefore, if a web page is added to the whitelist for embedded links, users can access all embedded web pages in the web page, simplifying the configuration.



- The whitelist for embedded links can be implemented in either of the following ways:
 - Use the manually configured referer-host to match the referer field in the HTTP request. If a match is found, the URL request is permitted. If no match is found, you can choose whether to match the referer field with all configured whitelist rules. After matching the referer field against the whitelist is enabled, the URL request is permitted if the referer field matches a whitelist rule.
 - After matching the referer field against the whitelist is enabled, the configured whitelist is directly used to match the referer field in the HTTP request. If a match is found, the URL request is permitted.
- The function of matching the referer field against the whitelist is enabled by default. You can disable this function as required.

URL Categories

- A large number of URLs can be classified into different categories. A URL category can contain multiple URLs. URL categories can be used to control a type of websites. URL categories are classified into predefined categories and user-defined categories. User-defined URL categories take precedence over predefined URL categories.
 - Predefined URL categories: Huawei maintains a large number of mainstream websites and classifies these websites. These websites are embedded in the firewall system and are called predefined URL categories, which are used to control access to common websites. Predefined URL categories cannot be created, deleted, or renamed.
 - User-defined URL categories are URL categories manually configured by the administrator. They are used to cover new websites and meet special filtering requirements.
- You can configure a user-defined URL category in either of the following ways:



Actions for URL Categories

- The firewall can perform different actions based on the URL category information.
 - Allow: allows user access to such websites.
 - Alert: allows user access and records logs.
 - Block: denies user access.
- To simplify operations, Huawei firewalls provide three default URL filtering levels and define the actions for each URL category.
 - High: Restricts access to websites related to pornography, illegitimate activities, social networking, and video sharing.
 - Medium: Restricts access to websites related to pornography and illegitimate activities.
 - Low: Restricts access to websites related to pornography.

URL Filtering Level				
Name	Allow	Alert	Block	Re-marked DSCP
User-defined Category Add ...	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	NONE
Abortion	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	NONE
Business/Economy/Finance	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	NONE
Advertisement	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	NONE
Bank	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	NONE
Industry/Agriculture	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	NONE
Insurance	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	NONE
Investment/Business	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	NONE

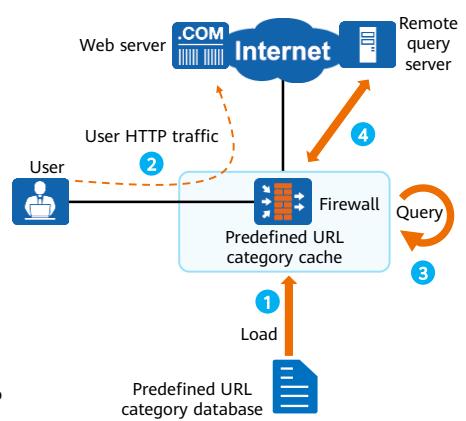
15 Huawei Confidential



- After the administrator uses the filtering level, the actions of all URL categories are automatically generated based on the filtering level.
- In a predefined category, the category also contains subcategories. However, in a security policy, the application of the processing action is always based on the subcategory. An enterprise administrator can set an action for a category so that all subcategories can inherit the action. An enterprise administrator can also adjust the action for a subcategory to meet differentiated management and control requirements. As shown in the figure, the IT-related category contains subcategories which inherit the processing action of the category. You can also set processing actions for subcategories separately.

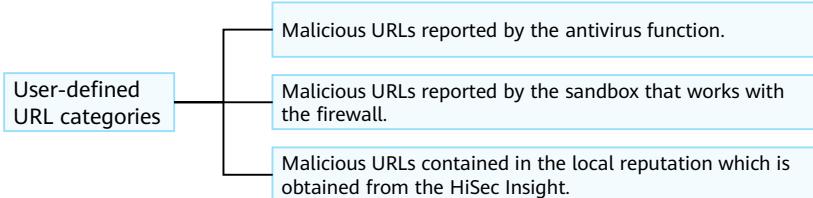
Process of Querying Predefined URL Categories

- Predefined URL categories can be queried in two modes: predefined URL category cache and remote query server. The process is as follows:
 - After the firewall is powered on, the predefined URL category database is automatically loaded to the predefined URL category cache. The predefined URL category database is preset before delivery and does not need to be manually loaded.
 - A user requests to access a URL resource. After receiving the request, the firewall extracts the URL information from the request packet.
 - The firewall queries the category to which the URL belongs in the predefined URL category cache. If the category is found, the firewall takes the action configured for the URL category.
 - If the category is not found, the firewall continues to query the category on the remote query server, processes the URL based on the query result, and saves the queried URL and its category information to the predefined URL category cache for quick query next time.



URL Reputation and Malicious URLs

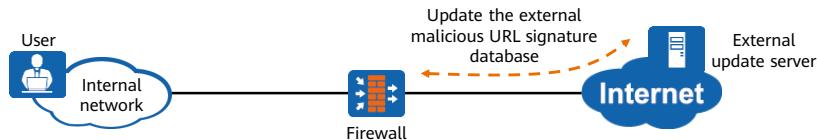
- URL reputation reflects the reliability of the URL that a user accesses. URL reputation values can be queried in two modes: URL reputation hotspot database and remote query server.
 - URL reputation hotspot database: The URL reputation hotspot database is released by sec.huawei.com. It is used to quickly obtain the latest URL reputation from the cloud to block untrusted URLs in a timely manner.
 - Remote query server: The URL reputation hotspot database update is disabled on the firewall and no URL reputation value is found in the predefined URL category cache. In this case, you can use the URL remote query function to obtain the latest URL reputation value.
- A malicious URL is a URL that contains malicious information. The sources of malicious URLs are as follows:



- A sandbox is a virtual system program that allows you to run browsers or other programs in a sandbox environment. Therefore, changes generated during the running can be deleted later. It creates a sandbox-like independent operating environment where programs running inside do not have a permanent impact on the hard drive. It is an independent virtual environment that can be used to test untrusted applications or online behaviors.
- Huawei's HiSec Insight is a big data-based advanced persistent threat (APT) defense product that helps with advanced threat analysis. It can effectively collect massive basic network data, such as traffic on the network, and network and security logs of various devices and perform real-time and offline big data analysis. Combined with machine learning technologies, expert reputation, and intelligence-driven technologies, HiSec Insight can effectively detect potential and advanced threats on the network to implement network-wide security situation awareness. In addition, HiSec Insight can work with Huawei HiSec solution to efficiently handle threats and prevent potential risks.

External Dynamic Malicious URL List

- The external dynamic malicious URL list is a text file of some malicious URLs released by external official websites. By updating the external malicious URL signature database, the firewall downloads the latest external dynamic malicious URL list from external official websites and loads it to its cache.
- After external dynamic malicious URL filtering is enabled, when a user requests to access a URL, the firewall matches the URL information with the external dynamic malicious URL list in the cache. If a match is found, the firewall directly blocks the URL request.
- The external malicious URL signature database supports only online update. Online update is classified into scheduled update and immediate update.



- Scheduled update:** Periodically connects to the external update server to check whether a new version of the external malicious URL signature database is available. If a new version of the external malicious URL signature database is available, the firewall automatically downloads and updates the local external malicious URL signature database at the specified time.
- Immediate update:** This update mode applies when a new external malicious URL signature database is detected on the network but the scheduled update time of the firewall is not reached or the scheduled update function is not enabled on the firewall. The download address for immediate update is the same as that for scheduled update, and the update processes in both modes are the same. The difference between two update modes is the update time. The immediate update can be implemented at any time.

URL Matching Rules (1/3)

- When filtering URLs based on the whitelist, blacklist, user-defined categories, and predefined categories, the firewall must comply with URL matching rules. There are four URL matching modes:

Matching Mode	Definition	Example
Prefix matching	Matches all URLs starting with a specified character string, such as www.example* .	To control access to all websites starting with www.example , configure the URL filtering rule www.example* .
Suffix matching	Matches all URLs ending with a specified character string, such as *aspx .	To control access to all image web pages at www.example.com , configure URL filtering rules *.jpg, *.jpeg, *.gif, *.png, and *.bmp .
Keyword matching	Matches all URLs containing a specified character string, such as *sport* .	To control access to all websites containing the word sport , configure the URL filtering rule *sport* .
Exact matching	The system checks whether a URL matches the specified string. If not, the system removes the last directory from the URL and matches the URL with the specified string. If the URL is still not matched, the system removes the last directory from the URL and matches the URL with the specified string. The process repeats until the URL contains only the domain name, for example, www.example.com.	To control the access to all websites at www.example.com , configure the URL filtering rule www.example.com .

- You can configure URL and host rules in the whitelist, blacklist, user-defined categories, and predefined categories. A URL rule matches all parts of a URL, whereas a host rule matches only a domain name (or IP address). The two types of rules apply to the following scenarios:
 - If the URLs to be permitted or blocked are domain names, both URL rules and host rules apply in most cases, and the two types of rules have the same filtering effect. For example, permit or block the access to domain name **www.example.com**.
 - If the permitted or blocked URLs are in the second-level domain name format and a small number of URLs need to be configured, either URL rules or host rules can be configured. If a large number of URLs need to be configured, configuring host rules is simple. For example, permit or block the access to domain name **news.example.com**.
 - If the permitted or blocked URLs carry directory and parameter information, only URL rules can be configured, and no host rule is suitable. For example, permit or block the access to URL **www.example.com/news**.

URL Matching Rules (2/3)

- URL matching modes are listed as follows in descending order of priority:
 - Exact matching > suffix matching > prefix matching > keyword matching
- For example, the URL **www.example.com/news** can match the following three modes at the same time. Based on the priority, the URL category corresponding to the exact matching condition **www.example.com/news** is used.
 - Exact matching: www.example.com/news
 - Prefix matching: www.example.com/*
 - Keyword matching: *example*
- In the same matching mode, a longer matching rule has a higher priority. For example, URL **www.example.com/news/index.html** first matches **www.example.com/news/*** in the following prefix matching rules:
 - www.example.com/news/*
 - www.example.com/*

URL Matching Rules (3/3)

- If the matching rules in the same mode have the same length, the configured action mode is used to determine the rule that a URL matches.
 - If the action mode is Strict, the URL category with the strictest action is used.
 - If the action mode is Loose, the URL category with the loosest action is used.
- As described in the following table, the two URL rules are in keyword matching mode and have the same length. For URL **www.example.com**, if two categories can be matched at the same time but the control actions are different:
 - If the action mode is Strict, the URL will match the category with a stricter action. In this example, the URL matches category B whose action is **Block**.
 - If the action mode is Loose, the URL will match the category with a looser action. In this example, the URL matches category A whose action is **Allow**.

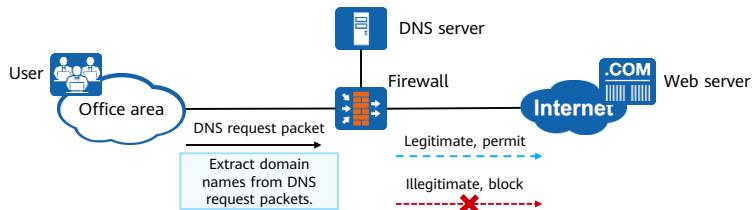
Category	Action
www.example.com/A	Allow
www.example.com/B	Block

Contents

1. Overview of Content Security Filtering Technologies
2. **Principles of Content Security Filtering Technologies**
 - URL Filtering
 - **DNS Filtering**
 - File Blocking
 - Data Filtering
 - Mail Filtering
 - Application Behavior Control
3. Examples for Configuring Content Security Filtering Technologies

Application Scenarios of DNS Filtering

- DNS filtering filters domain names in DNS request packets to allow or prohibit users' access to certain websites, regulating online behaviors.
- The firewall is deployed at the network border as the enterprise's gateway. When enterprise users initiate web requests, the firewall can allow, alert, or block users' requests by filtering domain names in the request packets.
- As shown in the following figure, DNS filtering is applied to:
 - Users' access requests to websites with legitimate domain names are permitted.
 - Users' access requests to websites with illegitimate domain names are blocked.



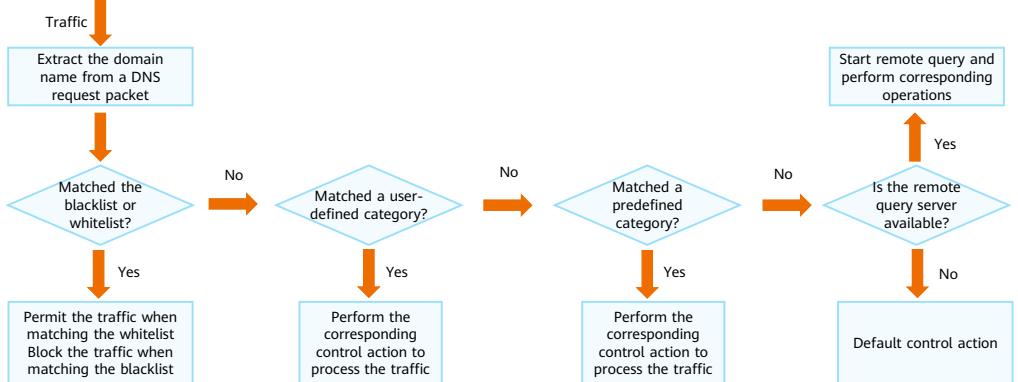
23 Huawei Confidential

 HUAWEI

- DNS filtering can allow or block requests based on the different schedules, user, or user group by referencing these configuration items to control users' Internet access permissions in a more refined and accurate manner.

Process of DNS Filtering

- If traffic matches a security policy that has a DNS filtering profile configured, the device extracts the domain name from the DNS request packet and sends the domain name for DNS filtering. The following figure shows the DNS filtering process:



24 Huawei Confidential

HUAWEI

- Similar to URLs, DNS categories may be user-defined or predefined. You can either create user-defined categories or use predefined categories to filter domain names.
- Predefined categories
 - A large number of common domain names are already added to predefined categories. You can easily manage the accessible and inaccessible domain name categories.
 - Predefined DNS categories are embedded in the system and are the same as predefined URL categories. You cannot create, delete, or rename predefined DNS categories, or add user-defined domain name rules to predefined DNS categories.
- User-defined categories
 - Although predefined categories cover mainstream websites, some new websites may not be covered. On the other hand, you can create user-defined categories to meet special filtering requirements or enhance predefined DNS categories.

Comparison Between URL Filtering and DNS Filtering

- The DNS filtering function filters domain names in DNS request packets to allow or prohibit users' access to certain websites, regulating their online behaviors. Compared with URL filtering, DNS filtering performs access control earlier, which effectively reduces the traffic of HTTP packets on the entire network.
- Compared with DNS filtering, URL filtering controls users' access to network resources in a more refined manner.

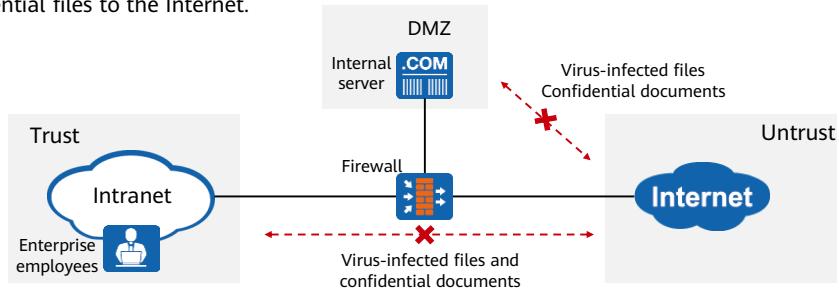
Item	URL Filtering	DNS Filtering
Access control phase	Perform the control when an HTTP/HTTPS URL request is initiated.	Perform the control in the domain name resolution phase.
Control granularity	Fine-grained. The control can be performed at the directory and file levels.	Coarse-grained. The control can be performed only at the domain name level.
Impact on performance	Big	Small
Control scope	Control only the HTTP/HTTPS access.	Control all services corresponding to the domain name.

Contents

1. Overview of Content Security Filtering Technologies
2. **Principles of Content Security Filtering Technologies**
 - URL Filtering
 - DNS Filtering
 - **File Blocking**
 - Data Filtering
 - Mail Filtering
 - Application Behavior Control
3. Examples for Configuring Content Security Filtering Technologies

Overview of File Blocking

- File blocking is a security mechanism used to filter files based on the file type. The firewall can block or generate alarms for specific types of files by identifying the file types.
- File blocking blocks the transmission of certain types of files, which reduces risks of executing malicious codes and viruses on the internal network and prevents employees from transmitting enterprises' confidential files to the Internet.



27 Huawei Confidential

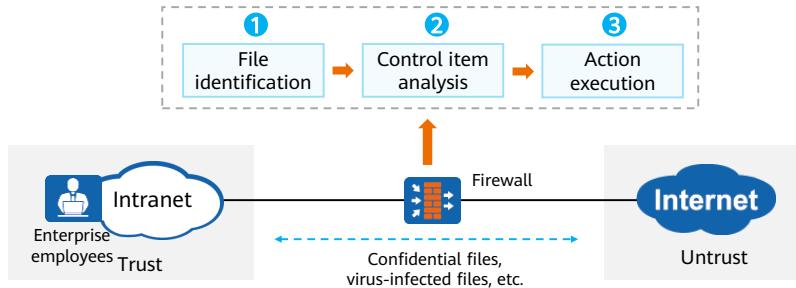
 HUAWEI

- The firewall identifies the types of files transferred through itself, and blocks or generates alarms for files of the specified type.
- If the file (traffic) that passes through the firewall matches a security policy rule, the action in the rule is permit, and the rule references the file blocking profile, file blocking detection is required.
- The administrator configures the file blocking function on the firewall to implement security protection as follows:
 - Reducing the risks of confidential information disclosure
 - Generally, the confidential information is stored in a document that can be compressed. If employees upload confidential documents to the Internet or hackers steal confidential documents from intranet servers, enterprises' confidential information or user information will be leaked. File blocking blocks the upload of documents and compressed files to the Internet and prevents Internet users from downloading documents and compressed files on the intranet server. Therefore, the risks of information leaks are greatly reduced.

- Reducing the risk of virus-infected files entering the internal enterprise network
 - Viruses often attach to executable files to evade detection and penetrate firewalls. File blocking prevents intranet users from downloading executable files from the Internet and blocks Internet users from uploading executable files to the intranet server. Therefore, the risks of virus infection are greatly reduced.
- Preventing file transfer that occupies bandwidth and affects employees' work efficiency
 - Downloading a large number of non-work-related video or image files does not only occupy network bandwidth but also reduce employees' work efficiency. Therefore, preventing intranet users from downloading video, image, and compressed files from the Internet ensures normal service bandwidth and employees' work efficiency.

Process of File Blocking

- After file blocking is configured on the enterprise gateway, files uploaded or downloaded by employees match the configured file blocking rules and the corresponding action is performed based on the identification result.



- Control items refer to the user-defined file type, file name extension, and file transfer direction. File analysis is performed based on these settings.

Principles of File Blocking Technologies (1/2)

- The firewall can identify received files as follows:
 - File application protocol: Files are transmitted over an application protocol, such as HTTP, FTP, SMTP, POP3, or IMAP.
 - File transfer direction: The value can be upload or download.
 - File type: The firewall can identify the actual file type. For example, the file name of **file.doc** can be changed to **file.exe**, but the file type is still .doc.
 - File name extension: It indicates the suffix of the file name (including the compressed file). For example, the file name extensions of **file.doc** and **file.exe** are .doc and .exe, respectively.
- If the firewall file identification result is abnormal, you need to configure the next action. Generally, the default value is used. The abnormal file type identification results are as follows:
 - Mismatched file name extension: The file type is inconsistent with the file name extension.
 - Unidentified file type: The file type cannot be identified and the file name extension is not available.
 - File damage: The file type cannot be identified because the file is damaged.

Principles of File Blocking Technologies (2/2)

- The firewall determines whether to match files with filtering rules as well as matching conditions based on file identification results and the action for file identification exceptions.

File Identification	Actions for File Identification Exceptions	Rule Matching
The file type and file name extension are consistent.	—	If the device matches the file with file blocking rules by type, the matching conditions are Application , Pre-defined file type , and Direction .
The file type and file name extension are inconsistent.	The device implements the action for the mismatched file name extension. <ul style="list-style-type: none">• Allow: allows file transfer and matches the file with the file blocking rules.• Alert: allows file transfer, records logs, and matches files with file blocking rules.• Block: blocks file transfer and records logs.	If the firewall matches the file with file blocking rules by type, the matching conditions are Application , File Type , and Direction .
The file type cannot be identified, but the file name extension exists.	—	If the device matches the file with file blocking rules by name extension, the matching conditions are Application , User-defined File Name Extension , and Direction .
The file type cannot be identified and no file name extension exists.	The device implements the action for the unidentified file type. <ul style="list-style-type: none">• Allow: allows file transfer.• Alert: allows file transfer and records logs.• Block: blocks file transfer and records logs.	—
The file is damaged.	The firewall implements the action for the damaged file. <ul style="list-style-type: none">• Allow: allows file transfer.• Alert: allows file transfer and records logs.• Block: blocks file transfer and records logs.	—

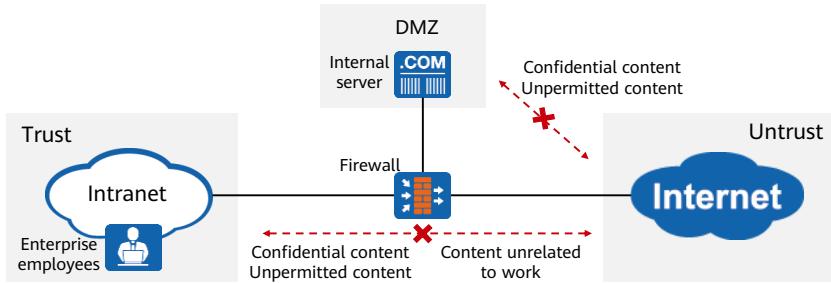
- The firewall sets an action for file identification exceptions and determines the next step based on the action.
- To match file blocking rules, the firewall matches file attributes (application, direction, file type, and file name extension) with the rules in the file blocking profile defined by the administrator.
 - If the attributes of a file meet all conditions in a file blocking rule, the file matches the rule successfully. Otherwise, the next rule is matched. If the file does not match any rule, the firewall allows the file transfer.
 - If the file matches a rule, the firewall implements the action defined in the rule. If the action is **Block**, the firewall blocks the file transfer. If the action is **Alert**, the firewall allows the file transfer and records a log.
- Note: If the file type cannot be identified, the system checks whether the file name extension exists. If the file name extension exists, the system matches the file against file blocking rules. If the file name extension does not exist, the system performs the action defined for files without file name extensions.

Contents

1. Overview of Content Security Filtering Technologies
2. **Principles of Content Security Filtering Technologies**
 - URL Filtering
 - DNS Filtering
 - File Blocking
 - **Data Filtering**
 - Mail Filtering
 - Application Behavior Control
3. Examples for Configuring Content Security Filtering Technologies

Introduction to Data Filtering

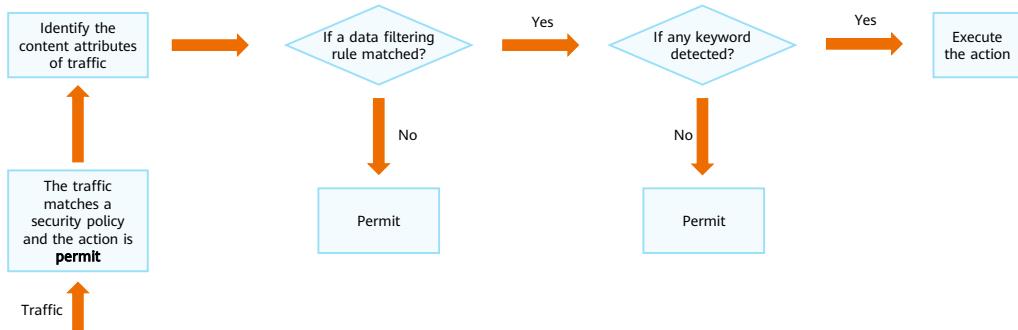
- Data filtering is a security mechanism that filters the content of a file or an application. The firewall implements in-depth identification of traffic content and performs the block or alert action on traffic containing specified keywords.
- Content filtering prevents disclosure of confidential information and transmission of violation information.



- The administrator configures the data filtering function on the firewall to implement security protection as follows:
 - Reduce the risks of enterprise confidential information disclosure.
 - Reduce legal risks because employees browse, release, or spread violation information.
 - Prevent employees from browsing and searching for content unrelated to work, improving working efficiency.

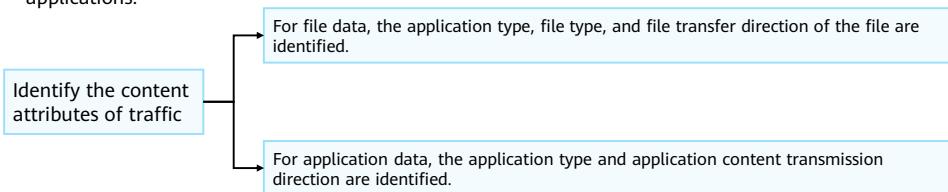
Process of Data Filtering

- If the traffic that passes through the device matches a security policy, the action in the security policy rule is **permit**, and the rule references the data filtering profile, data filtering detection is required for the traffic. The procedure is as follows:



Traffic Identification for Data Filtering

- The data filtering technology implements in-depth identification of traffic content and the device performs the block or alert action on traffic containing specified keywords. Data filtering falls into two types: file data filtering and application data filtering.
 - File data filtering filters the uploaded and downloaded files by keyword. You can specify the protocols for file transfer or the types of files to be filtered.
 - Application data filtering filters application content by keyword. The content filtered varies according to different applications.

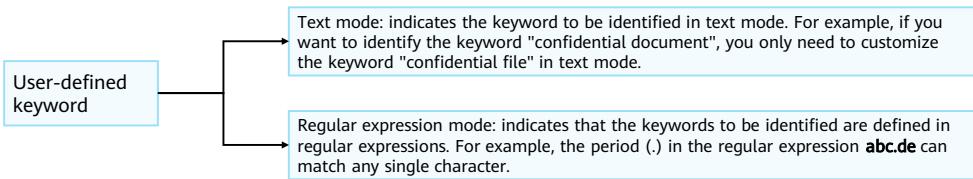


Filtering Content Supported by Common Protocols

Protocol	Supported Filtering Content
HTTP	Upload direction: content of microblogs posted by users, content of posts posted by users, content entered by users for search, content of information submitted by users, and names of uploaded files Download direction: content of browsed web pages, and names of files downloaded using HTTP
FTP	Names and content of uploaded and downloaded files
SMTP	Title, body, and attachment name of the sent mail
POP3	Title, body, and attachment name of the received email
IMAP	Title, body, and attachment name of the received mail
NFS	Content of the file uploaded or downloaded
SMB	Content of the file uploaded or downloaded

Keyword Detection for Data Filtering

- A keyword refers to the content to be identified by the device in data filtering. The device performs the specified action for the files or applications containing a specified keyword. Generally, the keyword is confidential or illegitimate information.
- The keyword includes pre-defined keywords and user-defined keywords.
 - Pre-defined keywords include bank card numbers, credit card numbers, social security numbers, ID card numbers, and confidentiality (including confidential, secret, and top secret information).
 - User-defined keywords can be texts or regular expressions.



- The following are common characters:
 - "." indicates that any non-line feed character is matched.
 - "()" indicates the start and end positions of a subexpression.
 - "*" indicates that the preceding character or expression is matched for zero or multiple times.
 - "\d" indicates that a digit is matched, ranging from 1 to 9.
 - "\w" indicates that digits, letters, and underscores (_) are matched.

Actions for Data Filtering

- When the device identifies keywords during data filtering detection, it performs a response action.

Action	Description
Alert	The device generates logs but does not block the content.
Block	The device blocks the content and generates logs. For users, the web pages cannot be displayed, files cannot be uploaded or downloaded, and mails cannot be sent or received.
Weight-based operations	Each keyword has a weight. The device adds the weights of identified keywords by matching count. If the sum of weights is less than the block threshold and greater than or equal to the alert threshold, the device generates an alarm. If the sum of weights is greater than or equal to the block threshold, the device blocks the traffic.

- The following is an example of weight-based operations:

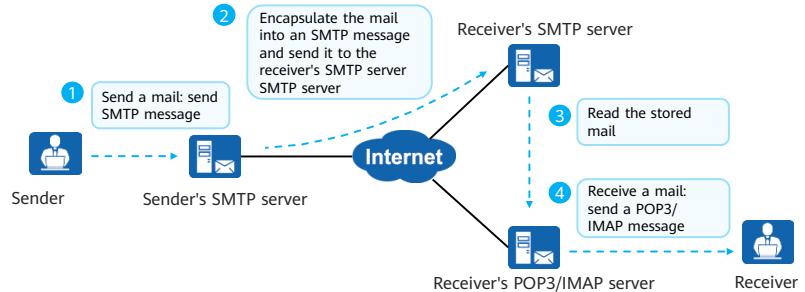
- Two keywords are defined on the device. The weight of keyword a is 1, and that of keyword b is 2. The alert threshold for data filtering is 1, and the block threshold is 5. Assuming that keyword a appears once on the web page browsed by a user, the sum of weights is 1, which is equal to the alert threshold. The device generates a log, but the user can continue browsing the web page. If keyword a appears three times and keyword b appears twice on the web page browsed by a user, the sum of weights is 7 ($3 \times 1 + 2 \times 2 = 7$), which is greater than block threshold 5. The device blocks the web page and generates a log, and the web page cannot be displayed for the user.

Contents

1. Overview of Content Security Filtering Technologies
2. **Principles of Content Security Filtering Technologies**
 - URL Filtering
 - DNS Filtering
 - File Blocking
 - Data Filtering
 - **Mail Filtering**
 - Application Behavior Control
3. Examples for Configuring Content Security Filtering Technologies

Process of Mail Transfer

- The following figure shows the mechanism for sending and receiving mails.
 - The user encapsulates the mail content into an SMTP message and sends it to the sender's SMTP server.
 - The sender's SMTP server encapsulates the mail into an SMTP message and sends it to the recipient's SMTP server for storage.
 - After receiving the request from the user, the POP3/IMAP server obtains the mail stored on the SMTP server.
 - The POP3/IMAP server encapsulates the mail into a POP3/IMAP message and sends it to the receiver.



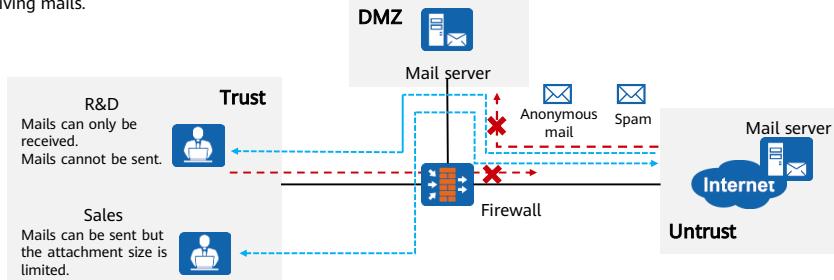
40 Huawei Confidential

HUAWEI

- The network administrator needs to deploy the SMTP and POP3 (or IMAP) services on the mail server, and mail client software (such as Microsoft Outlook or Foxmail) is installed on an end user's PC.
- Mail transfer protocols:
 - SMTP defines how PCs send mails to an SMTP server and how mails are transferred between SMTP servers.
 - Post Office Protocol 3 (POP3) and Internet Mail Access Protocol (IMAP) specify how PCs manage and download mails on the mail server through client software.
 - The differences between IMAP and POP3 are as follows: When POP3 is used, after the client software downloads unread mails to the PC, the mail server deletes the mails. If IMAP is used, users can directly manage mails on the server without downloading all mails to the local PC.

Overview of Mail Filtering

- Mail filtering manages and controls the mail receiving and sending behavior, including preventing flooding of spam and anonymous mails and controlling unauthorized mail receiving and sending.
- Mail filtering checks IP addresses and filters mail content to enhance mail system security for LAN users.
 - The IP address check prevents flood of spam on the intranet.
 - Mail content filtering filters out anonymous mails and checks mail content to control permission of intranet users for sending or receiving mails.



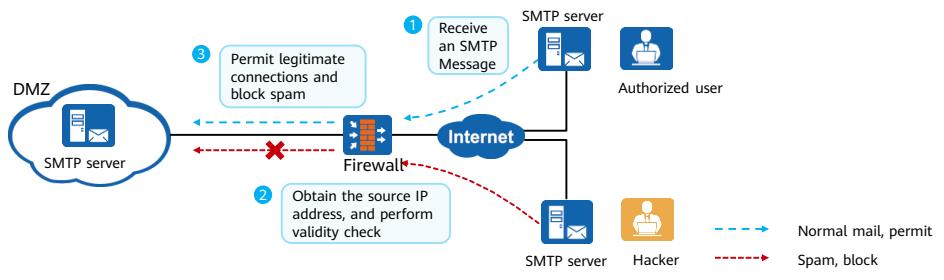
41 Huawei Confidential

 HUAWEI

- As shown in the figure, the firewall functions as the security gateway of an office network and the mail server is deployed on the intranet. Intranet users send and receive mails through the intranet mail server.
- After mail filtering is configured on the firewall, the following mail security protection can be implemented:
 - Enable the anti-spam function to prevent the intranet SMTP server from receiving a large amount of spam.
 - Enable the anonymous mail check function to prevent illegitimate information from being transmitted over the entire network in anonymous mails.
 - Enable the mailbox address check function. In this way, only the specified mail address can be used to send or receive mails. With the mail sending and receiving permissions being controlled, important information disclosure by intranet users can be prevented.
 - Enable the mail attachment control function to control the size and number of attachments, preventing a large amount of information from being leaked through attachments.

IP Address-based Filtering (1/2)

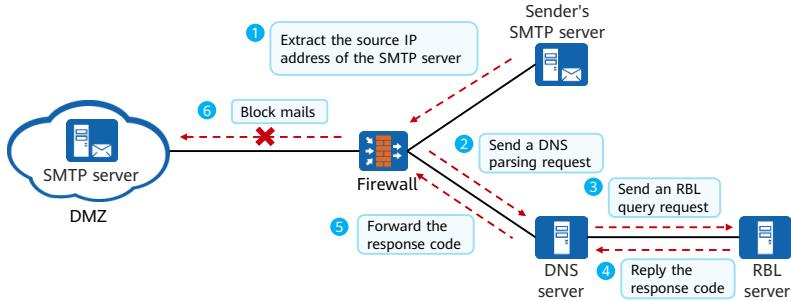
- According to the mail working mechanism, no authentication is performed between the PC and the mail server or between the mail servers. Attackers can send mails through any SMTP server on the Internet.
- To prevent spam flooding, you can check the validity of the source IP address of the sender's SMTP server.
 - Query the local blacklist and whitelist
 - Query the Real-time Blackhole List (RBL)



- The RBL is a large online database jointly collected anti-spam organizations and lists the IP address of the SMTP servers that frequently forward spam.
- Spam refers to a mail that is sent to a user's mailbox without permission. The spam usually contains advertisements, publicity materials, or even virus programs. A large amount of spam not only consumes network bandwidth, occupies mailbox space, but also brings security risks.
- In IP address check, the firewall checks the source IP address of the sender's SMTP server. The implementation process is as follows:
 - The firewall receives SMTP messages from other SMTP servers, including normal mails and spam.
 - The firewall checks the IP address.
 - Parses the SMTP message and obtains the source IP address of the sender's SMTP server from the SMTP message.
 - Checks the validity of the source IP address. The firewall compares the IP address with the blacklist and whitelist to determine the validity of the IP address:
 - If the source IP address matches the local whitelist, the mail is legitimate. Otherwise, the mail is searched against the local blacklist.
 - If the mail matches the local blacklist, the mail is considered as spam. Otherwise, the mail is searched against the RBL.
 - If the mail matches the RBL, the mail is spam. Otherwise, the mail is legitimate.
 - Allows legitimate mails and blocks spam.

IP Address-based Filtering (2/2)

- RBL query mechanism:
 - The firewall obtains the IP address of the sender's SMTP server and sends a query request to the RBL server.
 - The RBL server maintains a real-time blacklist. All SMTP servers in the blacklist have sent spam.
 - The firewall determines whether the IP address belongs to the spam server based on the result returned by the RBL server and takes the corresponding actions.



43 Huawei Confidential

HUAWEI

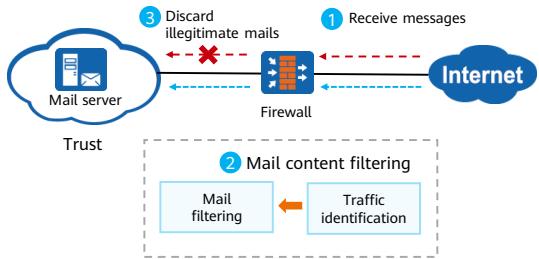
- The query process is as follows:

- 1 After receiving an SMTP message, the firewall extracts the IP address of the sender's SMTP server.
- 2 The firewall adds the IP address parsed in the preceding step and the RBL service name specified by the third-party RBL server to a message and sends a parsing request to the DNS server. For example, if the source IP address of the SMTP server is 1.2.3.4 and the RBL service name is **sbl.spamhaus.org**, the firewall sends **4.3.2.1.sbl.spamhaus.org** to the DNS server.
- 3 The DNS server reads the RBL service name in the received message, parses the IP address of the RBL server, and forwards the query request to the RBL server.
- 4 After receiving the query request, the RBL server returns an IP address as a response code to the DNS server. The response code indicates whether an IP address is found for this RBL query.
- 5 The DNS server forwards the response code obtained from the RBL server to the firewall.
- 6 The firewall determines whether the mail sent by the SMTP server is spam based on the response code.
 - If the response code obtained from the RBL server is the same as that configured on the firewall, the SMTP mail is regarded as spam.
 - If the response code obtained from the RBL server is different from that configured on the firewall, the SMTP mail will be allowed to pass through.

Mail Content-based Filtering

- When the firewall functions as the security gateway, all data information must be forwarded by the firewall. Before forwarding the information, the firewall checks the information and filters out the information that contains illegitimate mails. The implementation process is as follows:

- The data reaches the firewall.
- The firewall performs mail content filtering.
 - Traffic identification: The firewall identifies mail content to be filtered based on the matching conditions, such as the source security zone, destination security zone, source IP address, and destination IP address.
 - Mail filtering: The firewall analyzes which traffic contains mail content, checks the mail address and attachment size, and identifies illegitimate mails.
- Discard the messages containing illegitimate mails.



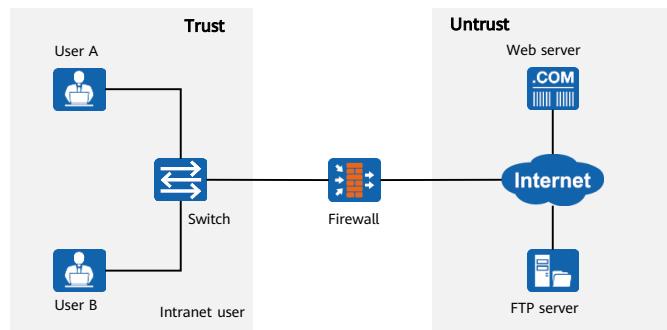
- Anonymous mail check, mail address check, and mail attachment control filter out illegitimate mails based on their content. They check the mail addresses of the sender and receiver, the attachment size, and the number of attachments.
- The mail content filtering detection is classified into the sending direction and receiving direction.
 - If the mail content is encapsulated in an SMTP message, the firewall performs detection in the sending direction.
 - If the mail content is encapsulated in a POP3 or an IMAP message, the firewall determines that the mail is in the receiving direction and performs detection in the same direction.

Contents

1. Overview of Content Security Filtering Technologies
2. **Principles of Content Security Filtering Technologies**
 - URL Filtering
 - DNS Filtering
 - File Blocking
 - Data Filtering
 - Mail Filtering
 - Application Behavior Control
3. Examples for Configuring Content Security Filtering Technologies

Application Scenarios of Application Behavior Control

- Enterprises need to manage HTTP and FTP behaviors of intranet users, and grant different permissions for different users to access network resources through HTTP and FTP and also for one user to access network resources at different schedules.
- The application behavior control function of the firewall can accurately control users' HTTP, FTP, and IM behaviors to meet the preceding requirements.



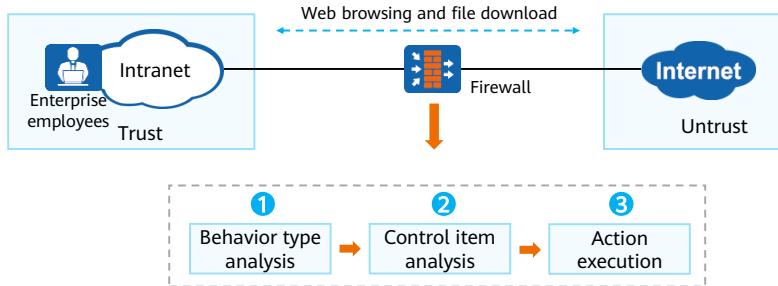
46 Huawei Confidential

 HUAWEI

- The firewall functions as an egress gateway of the enterprise and is deployed at the intranet egress. The application behavior control function is deployed on the firewall to effectively manage the HTTP, FTP and IM behaviors of intranet users when they access the Internet.
- Multiple application behavior control profiles are created on the firewall. Each profile is used to grant different HTTP, FTP and IM permissions to intranet users. Then objects such as the profiles, users, and schedules (working hours and non-working hours) are referenced in security policies to deliver differentiated and fine-grained control on HTTP, FTP and IM behaviors of intranet users.

Process of Application Behavior Control

- Traditional devices control HTTP and FTP behaviors by protocol or port. However, the firewall can implement more refined control over HTTP and FTP behaviors.
- As shown in the figure, the firewall analyzes the behavior type, performs the action corresponding to the application behavior control item, and even performs control based on different users and schedules.



HTTP-based Behavior Control Technologies

Behavior Type	Control Item	Description	Action
HTTP behavior	POST	The POST method of HTTP is commonly used to send information to the server through web pages. For example, you are using this method when you post on BBS, submit forms, and use your user name and password to log in to a specific system.	Permit/Deny
	Web browsing	You can use a web browser to browse web pages.	
	Internet access using a proxy	You can use a proxy server to access specified websites. To implement this function, you must deploy the firewall between the intranet and the proxy server.	
	File upload/download	Uploads or downloads files.	Alert/Block
	Size of the posted content in HTTP POST operations (Alert/Block threshold)	When HTTP POST is permitted, you can configure an alert threshold and a block threshold to control the POST operation content size.	
	Upload/Download file size (Alert/Block threshold)	When file upload is allowed, you can configure an alert threshold and a block threshold to control the file size.	

- Alert threshold: When the size of the file to be uploaded or downloaded (or the size of the POST operation content reaches the alert threshold), the system generates a log and displays it to the administrator.
- Block threshold: When the size of the uploaded or downloaded file or the size of the POST operation content reaches the block threshold, the system blocks the uploaded or downloaded file or POST operation and generates a log to notify the device administrator.
- When you create security policies, you can combine the application behavior control profile and objects such as the user and schedule to implement differentiated management of users in different schedules.

FTP-based Behavior Control Technologies

Behavior Type	Control Item	Description	Action
FTP behavior	File upload	You can set an alarm threshold and a block threshold to limit the size of the upload file if file upload is allowed.	Permit/Deny
	File download	You can set an alarm threshold and a block threshold to limit the size of the download file if file download is allowed.	
	File deletion	You can delete a file from the FTP server.	

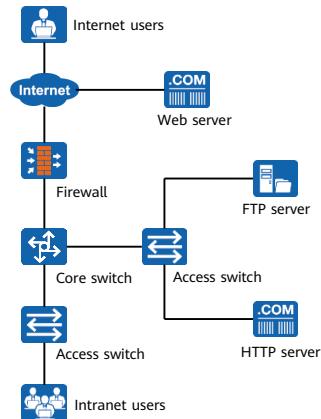
- By default, no alarm threshold or block threshold is configured, and the system does not control the size of the uploaded or downloaded file or the content size of the POST operation
- The alarm threshold and block threshold can be separately or both configured. If both thresholds are configured, ensure that the alarm threshold is lower than the block threshold.

Contents

1. Overview of Content Security Filtering Technologies
2. Principles of Content Security Filtering Technologies
3. **Examples for Configuring Content Security Filtering Technologies**

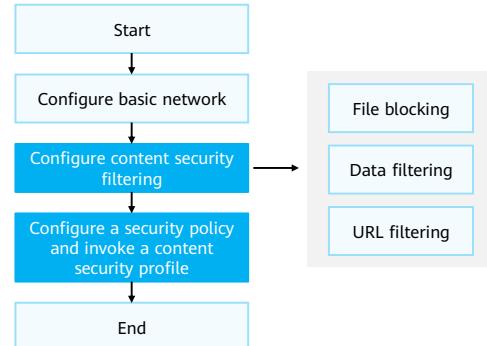
Example for Configuring Content Security - Requirement Description

- An enterprise has deployed a firewall as a security gateway at the intranet egress. In addition to normal network running, the enterprise requires:
 - Prohibit employees from uploading executable files to the intranet server to reduce the risk of viruses entering the intranet.
 - Prevent internal employees from disclosing confidential information while ensuring normal network usage.
 - A website **www.example.com** is suspected to have security risks. Intranet employees cannot access this website or social network websites.



Example for Configuring Content Security - Configuration Roadmap

- Configuration roadmap:
 - Configure IP addresses and routes for devices to ensure interconnection.
 - Configure file blocking to prevent employees from uploading suspicious files.
 - Configure data filtering to prevent employees from disclosing confidential information.
 - Configure URL filtering to prevent employees from accessing unpermitted websites.
 - Configure URL remote query to expand the local predefined URL category database for quick query.
 - Configure a security policy and invoke the content security profile.



Configuring File Blocking

- Choose **Object > Security Profile > File Blocking** and set the parameters as follows:
 - Create the file blocking profile **profile_file_1**.
 - Create file blocking rule **rule1** and configure a policy to block the upload of executable files.

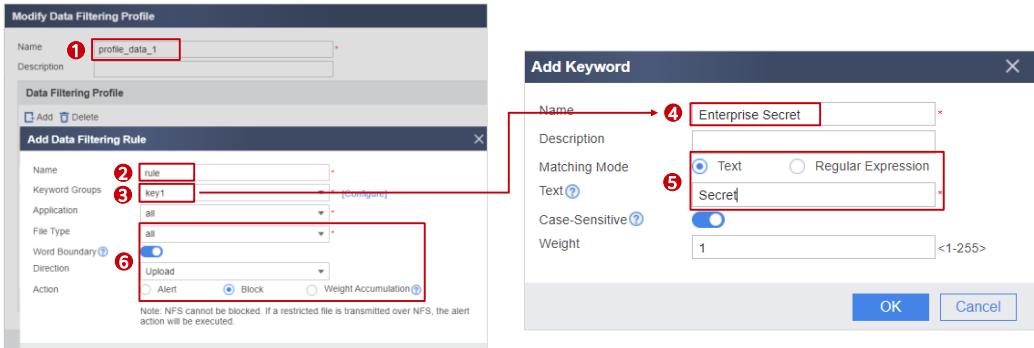
The image contains two screenshots of a software interface for managing file blocking profiles and rules.

Add File Blocking Profile: This screenshot shows the configuration of a new profile. The 'Name' field is filled with 'profile_file_1'. The 'File Blocking Rules' section is empty, indicated by a red box labeled '1'.

Add File Blocking Rule: This screenshot shows the configuration of a new rule named 'rule1'. It includes fields for 'Application' (set to 'all'), 'File Type' (set to 'DOC,PPT,XLS,MSOFFICE,DOCX,PPT;'), 'Direction' (set to 'Upload'), and 'Action' (set to 'Block'). A note at the bottom states: 'Note: NFS cannot be blocked. If a restricted file is transmitted over NFS, the alert action will be executed.' Red boxes labeled '2' and '3' highlight the 'File Type' and 'Action' fields respectively.

Configuring Data Filtering

- Choose **Object > Security Profile > Data Filtering** and set the parameters as follows:
 - Create data filtering profile **profile_data_1** and data filtering rule **rule**.
 - Create keyword group **key1** and keyword **Enterprise Secret** to match the text **Secret**.



Configuring URL Filtering (1/2)

- Choose **Object > Security Profiles > URL Filtering**, create a URL filtering profile, and set the filtering level to **User-defined**.

The screenshot shows the configuration page for a URL filtering profile named "untrust_url". The profile includes settings for encrypted traffic filtering and malicious URL detection. It features two tabs: "Whitelist" and "Blacklist", both of which are currently empty. Below these tabs is a section titled "URL Filtering Level" where the "User-defined" option is selected.

Name	① untrust_url	
Description		
Filter Encrypted Traffic	<input type="checkbox"/> This function facilitates URL filtering on encrypted HTTPS traffic.	
Default Action	Allow	
Malicious URL Detection	<input type="checkbox"/> This function blocks access to malicious URLs. Enabling remote URL query further enhances its effectiveness.	
Type	Whitelist	Blacklist
URL	Whitelist entries take precedence over blacklist entries.	Whitelist entries take precedence over blacklist entries.
Host	Whitelist entries take precedence over blacklist entries.	Whitelist entries take precedence over blacklist entries.
URL Filtering Level		
<input type="radio"/> High	Restricts access to websites related to pornography, illegal activities, social networking, and video sharing.	
<input type="radio"/> Medium	Restricts access to websites related to pornography and illegal activities.	
<input type="radio"/> Low	Restricts access to websites related to pornography.	
<input checked="" type="radio"/> ② User-defined		

Configuring URL Filtering (2/2)

- Set the action (**Allow**, **Alert**, or **Block**) for the URL category as required, create the URL category **untrust**, match URL **www.example.com**, and set the action to **Block**.

The screenshot shows two windows related to URL filtering configuration:

- Top Window (List of Categories):** A table with columns: Name, Action (Allow, Alert, Block), and Re-marked DSCP (NONE). It lists several categories:
 - User-defined Category [Add URL Category] (highlighted with a red box and number 3): Action is Block.
 - Abortion: Action is Block.
 - Business/Economy/Finance: Action is Block.
 - Crime: Action is Block.
 - Cult: Action is Block.
- Bottom Window (Add URL Category Dialog):** A modal dialog with fields: Name (untrust), Description (empty), and URL (www.example.com). The URL field is highlighted with a red box and number 4.

Configuring URL Remote Query (1/2)

- To ensure that the local firewall can communicate with the remote server, you need to configure security policies to allow the traffic of the services to pass through the firewall:
 - Choose **Object > Service > Service** to create a user-defined service.
 - Choose **Policy > Security Policy > Add Security Policy** and reference the user-defined service.

The image shows two side-by-side configuration screens. The left screen is for creating a user-defined service named 'service_sec_huawei_com'. It includes fields for Name (1), Description, Session Timeout (<1-65535>s), and a Protocol List table with three entries (2). The right screen is for adding a security policy. It shows General Settings (4) with 'Name' set to 'policy_sec_huawei_com' and 'Tag' set to 'local' (5). Under Source and Destination, 'Source Zone' is 'local' and 'Destination Zone' is 'untrust'. Under User and Service, 'Service' is selected (6) and the value is 'service_sec_huawei_com'.

Protocol Number	Source Port	Destination Port	ICMP	Type
6 (TCP)	0-65535	80	---	---
6 (TCP)	0-65535	12612	---	---
17 (UDP)	0-65535	12600	---	---

57 Huawei Confidential

HUAWEI

- To use the URL remote query service, ensure that the following operations have been performed:
 - The license has been activated and is within the valid service period.
 - The firewall is reachable to sec.huawei.com.
 - A DNS server address is configured, and the DNS server can correctly resolve the domain name sec.huawei.com.
- Note: sec.huawei.com is the website of Huawei security center platform.

Configuring URL Remote Query (2/2)

- Set the parameters of the URL remote query server.
 - Choose **Object > Security Profiles > Global Configuration**.

The screenshot shows the 'Global Configuration' page with the following settings:

- File blocking have changed, Click Commit to apply the changes.**
- Disable Resumable Downloading:** FTP HTTP
- Country:** CHINA (selected)
- File Decompression:**
 - Maximum Layers: 3
 - Action: Allow
 - Maximum File Size: 100
 - Action: Allow
- File Reputation Server Settings:**
 - Query Mode: Remote Local
 - Scheduling Center: sec.huawei.com

Three numbered callouts point to specific fields:

- ① Points to the 'CHINA' dropdown under 'Country'.
- ② Points to the 'Remote' radio button under 'Query Mode'.
- ③ Points to the 'Apply' button at the bottom right.

Referencing a Content Security Profile

- Choose **Policy > Security Policy > Security Policy > Add Security Policy**.
 - Set the security policy name to **to_Internet**, configure the source and destination security zones, and reference a content security profile.

The screenshot shows the 'Add Security Policy' configuration interface. It is divided into several sections:

- General Settings:** Name is set to **to_Internet** (highlighted with red box 1).
- Source and Destination:** Source Zone is set to **trust** (highlighted with red box 2). Destination Zone is set to **untrust**.
- User and Service:** Destination Address/Region is set to **10.0.11.0/24**.
- Content Security:** The 'Content Security' section is expanded, showing various security profiles. The **untrust_url** profile is highlighted with red box 3.

Quiz

1. (True or false) When the HTTP file download action is set to **Deny**, you can set the block threshold. ()
 - A. True
 - B. False
2. (Multiple-answer question) Which of the following are content security filtering technologies? ()
 - A. File blocking
 - B. Data filtering
 - C. Mail filtering
 - D. Application behavior control

1. B
2. ABCD

Summary

- This course describes the functions related to content security filtering. By deploying the content security filtering function on the firewall, you can implement refined management and control on enterprise users. For example, access to illegitimate websites is not allowed to prevent adverse impacts on enterprises, access to entertainment websites during working hours is not allowed to improve work efficiency, and core confidential information leakage is prevented.
- Upon completion of this course, you have understood the implementation of content security filtering technologies and been able to independently configure URL filtering, file blocking, and data filtering on Huawei firewalls.

Recommendations

- Huawei official websites:
 - Enterprise service: <https://e.huawei.com/en/>
 - Technical support: <https://support.huawei.com/enterprise/en/index.html>
 - Online learning: <http://learning.huawei.com/en/>

Acronyms and Abbreviations

Acronym/Abbreviation	Full Name
DNS	Domain Name Service
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IM	Instant Messaging
IMAP	Interactive Mail Access Protocol
NFS	Networked File System
POP3	Post Office Protocol 3
RBL	Real-time Blackhole List
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
URL	Uniform Resource Locator

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。
Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

Copyright©2022 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product performance, market position, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.



Emergency Response



Foreword

- The development of emerging technologies such as the Internet of Things (IoT), mobile Internet, cloud computing, big data, and blockchain injects new vitality into the entire IT industry, improves production efficiency, and brings convenience to life. However, the emergence of new technologies also provides new attack methods and channels for cyber attacks. The attack scope expands year by year, causing increasingly serious impacts and bringing new challenges to cyber security.
- There is no absolutely secure system, and there is no absolutely secure network. Facing the complex and ever-changing network environment, it is an urgent need to establish an effective emergency response mechanism to ensure the cyber security of enterprises and organizations and protect enterprise data assets.
- This course describes the processes and technologies related to the cyber security emergency response.

Objectives

- Upon completion of this course, you will be able to:
 - Describe the basic concepts of cyber security emergency response.
 - Describe the handling process of cyber security emergency response.
 - Understand technologies related to cyber security emergency response.

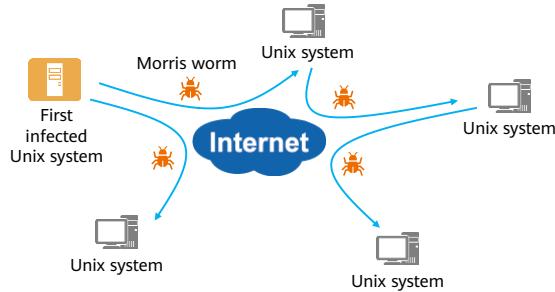
- In the following text, "cyber security emergency response" is referred to as "emergency response".

Contents

- 1. Emergency Response Overview**
2. Emergency Response Process
3. Emergency Response Technologies and Cases

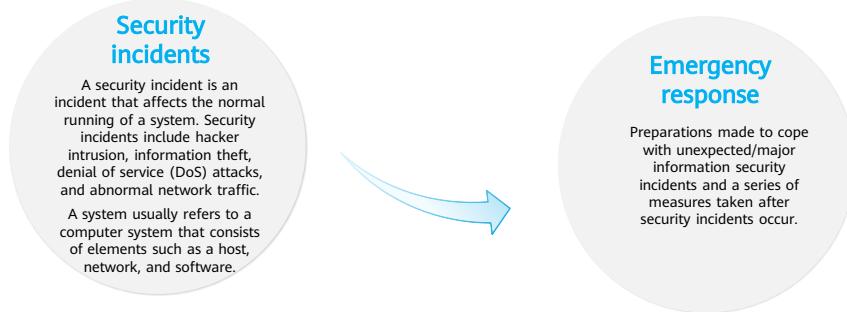
Background

- The Morris Worm Incident, which occurred in November 1988, forced over 10% Internet systems to stop working. This incident shocked the world and deeply concerned computer science professionals.
- Following this incident, in 1989, the Defense Advanced Research Projects Agency (DARPA) sponsored Carnegie Mellon University's Software Engineering Institute (SEI) for developing a communication coordination center — the Computer Emergency Response Team (CERT) and the CERT Coordination Center (CERT/CC) to help defend against cyber attacks.



What Is Emergency Response?

- Emergency response is a task that requires full preparation and refined organization. During the emergency response process, incorrect operations, actions that may cause catastrophic consequences, or skipping of key steps must be avoided.
- The objectives of emergency response include: taking emergency measures and actions to restore services; investigating the causes of security incidents to prevent similar security incidents from happening again; providing digital evidence recognized by laws for judicial authorities if necessary.



5 Huawei Confidential

 HUAWEI

- Related standards:

- GB/T 24363-2009 Information Security Technology — Information Security Emergency Response Plan Specifications
- GB/T 20985.1-2017 Information Technology — Security Technology — Information Security Incident Management Guide — Part 1: Incident Management Principles
- GB/T 20985.2-2020 Information Technology — Security Technology — Information Security Incident Management Guide — Part 2: Guidelines for Incident Response Planning and Preparation
- GB/Z 20986-2007 Information Security Technology — Guidelines for the Category and Classification of Information Security Incidents
- GB/T 20988-2007 Information Security Technology — Disaster Recovery Specifications for Information Systems

Contents

1. Emergency Response Overview
- 2. Emergency Response Process**
3. Emergency Response Technologies and Cases

Emergency Response Phases

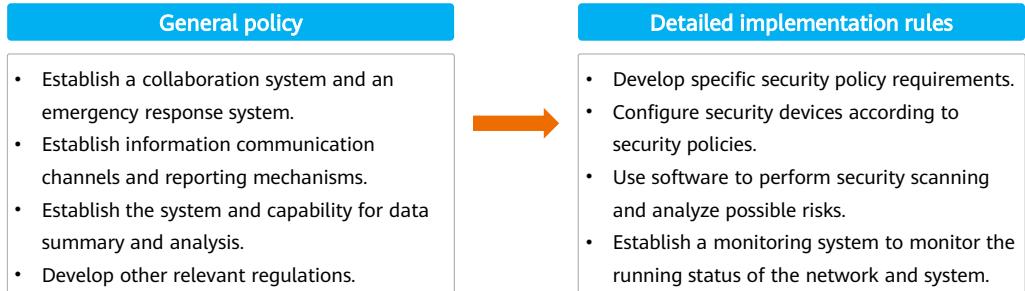
- Cyber security emergency response can quickly and efficiently trace, handle, and prevent cyber security incidents to ensure network information security. The cyber security emergency response process can be divided into the following phases:

Preparation	Identification	Containment	Eradication	Recovery	Lessons Learned
<ul style="list-style-type: none">• Reach a consensus.• Establish an emergency response process.• Set up an emergency response team.	<ul style="list-style-type: none">• Keep identifying and monitoring to check whether security incidents occur.• Evaluate risks, impacts, and losses.	<ul style="list-style-type: none">• Control the impact scope of security incidents to avoid incident escalation.• Perform containment operations, such as blocking IP addresses.	<ul style="list-style-type: none">• Find out the root cause.• Remove vulnerabilities, Trojan horses, and viruses.	<ul style="list-style-type: none">• Restore service continuity.• Backup data.• Delete the temporary policies.	<ul style="list-style-type: none">• Output the overall emergency response report.• Pick out problems and make improvements.• Summarize experience.

- The emergency response process varies according to situations. The emergency response service personnel need to flexibly handle security incidents but must record all process changes.
- Reference files:
 - GB/T 20984-2007 Information Security Technology — Risk Assessment Specification for Information Security
 - GB/T 20985.1-2017 Information Technology — Security Technology — Information Security Incident Management Guide — Part 1: Incident Management Principles
 - GB/T 20985.2-2020 Information Technology — Security Technology — Information Security Incident Management Guide — Part 2: Guidelines for Incident Response Planning and Preparation
 - GB/Z 20986-2007 Information Security Technology — Guidelines for the Category and Classification of Information Security Incidents
 - GB/T 20988-2007 Information Security Technology — Disaster Recovery Specifications for Information Systems
 - GB/T 22239-2019 Information Security Technology — Baseline for Classified Protection of Cybersecurity
 - GB/T 22240-2020 Information Security Technology — Classification Guide for Classified Protection of Cybersecurity

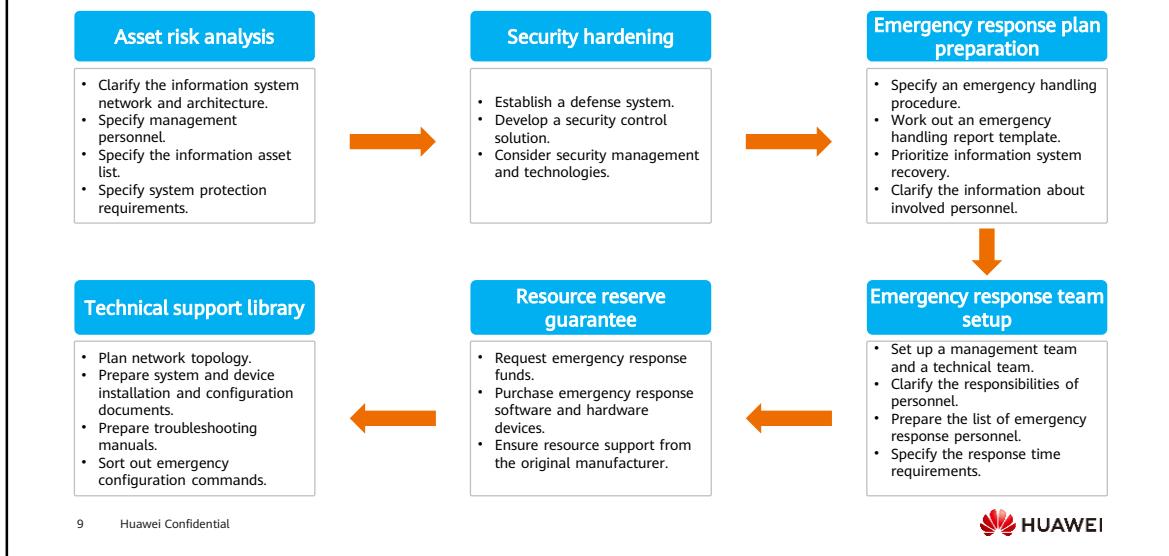
Preparation

- Before a cyber security incident occurs, evaluate possible security incidents and develop corresponding emergency policies and plans.



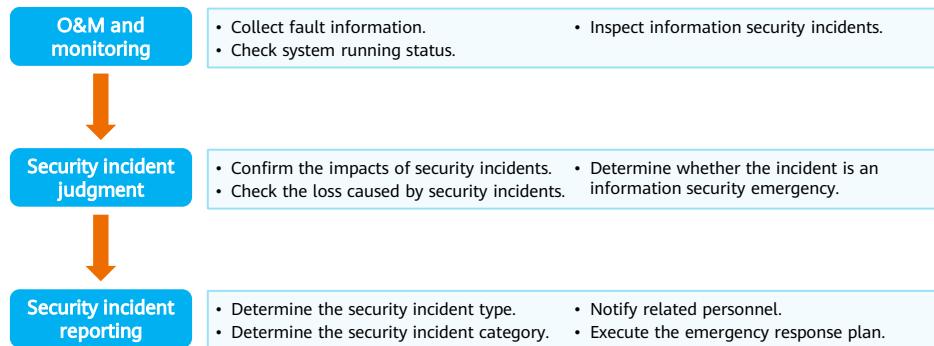
- In the preparation phase, we need to customize a detailed emergency response plan and prepare resources accordingly. For example:
 - Personnel: emergency operation personnel, technical experts, and the support personnel from hardware vendors and software system vendors.
 - Deploy related software and hardware devices (security devices) for security detection and subsequent source tracing analysis.
 - Service continuity assurance: Build a disaster recovery (DR) system for services.

Detailed Rules for the Preparation



Identification

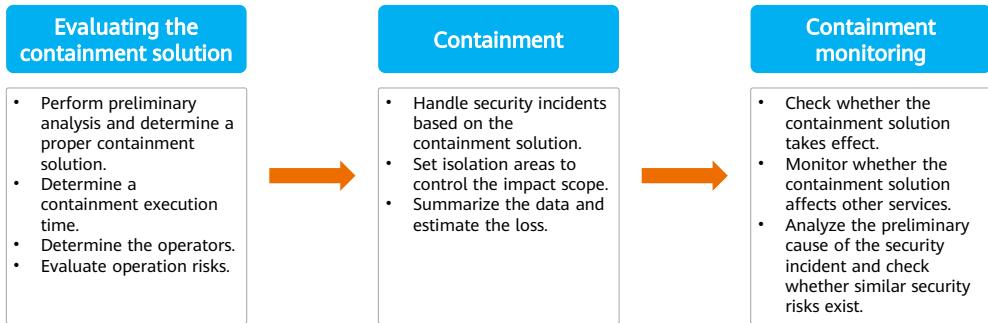
- Identify and confirm the occurrence of security incidents and determine the category and impact of the incidents.
- The general identification process is as follows:



- Identification: Create security warning reports before emergency security incidents. In case of an emergency, report a security warning to the emergency response center. The emergency response center takes the corresponding measures based on the incident severity.
- In the identification phase, we determine whether security incidents occur based on symptoms such as abnormal service system access, abnormal network traffic, and a large number of suspicious emails. In addition, technical measures, security detection devices (such as IPS and sandboxes), antivirus software on the host, and service host logs are used to make comprehensive judgment.

Containment

- In the containment phase, take necessary measures from multiple aspects to confine network attacks within a certain range, reducing losses.
- When a security incident occurs, start the emergency response plan and take emergency measures based on the preset rules. The containment procedure is as follows:



11 Huawei Confidential



- Take different containment actions in different scenarios. Common containment actions are as follows:
 - Determine a proper containment method, such as blocking attacks, mitigating system loads, blocking the intrusion source address using routers and firewalls, and isolating the systems infected by viruses.
 - Modify the filtering rules of all firewalls and routers to deny the traffic from suspicious hosts.
 - Block or delete the attacked login accounts.
 - Raise system or network behavior monitoring levels.
 - Set honeypots, and disable the exploited services.
 - Summarize data to estimate the loss and isolation effect.

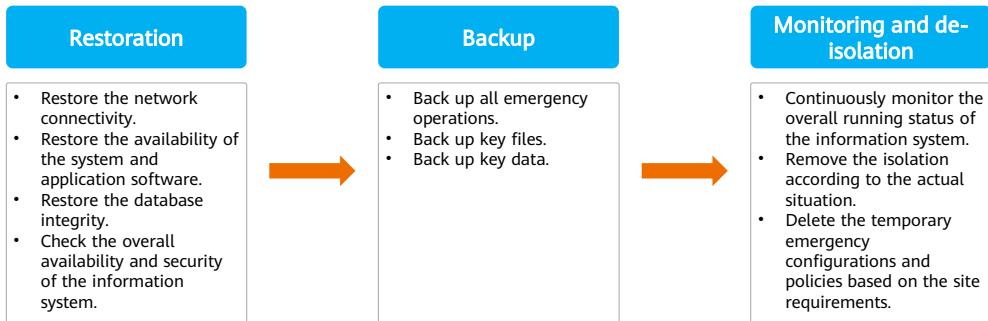
Eradication

- Find out the root cause of the security incident and take corresponding measures to eliminate similar security risks.
- The general process is as follows:



Recovery

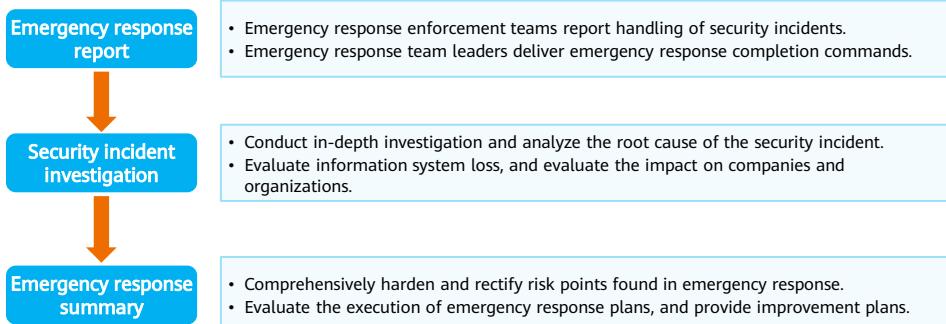
- Restore the intruded and damaged information assets such as networks, systems, applications, and databases, and back up and de-isolate them in a timely manner.
- The specific tasks in the recovery phase are as follows:



- The recoverability depends on the preparations, damage caused by attacks, and backup status of the information system.

Lessons Learned

- Learn lessons from security incident responses, and summarize information about security incidents.
- The specific tasks in the lessons learned phase are as follows:



Contents

1. Emergency Response Overview
2. Emergency Response Process
3. **Emergency Response Technologies and Cases**
 - Emergency Response Technologies
 - Emergency Response Cases

Emergency Response Technologies

- Emergency response technologies refer to the technologies and methods used in responding to network attack events.
- Emergency response technologies are required in the identification, containment, eradication, and recovery phases of the emergency response process. Common emergency response technologies are as follows:

Checking files

- Check whether there are abnormal files left by attackers or check key system files to determine whether the service host is intruded.

Checking processes

- Check whether abnormal processes exist to determine whether the service host is intruded, or implanted with a Trojan horse/backdoor.

Checking system information

- Check the environment variables and scheduled tasks of the system to determine whether variables and tasks added by attackers exist.

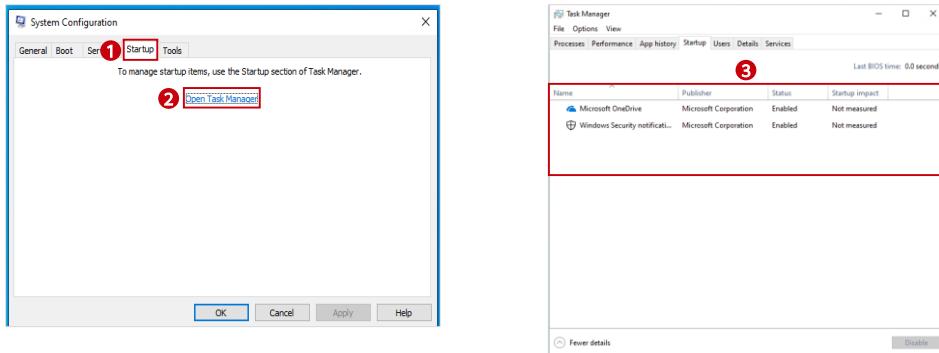
Log analysis

- Analyze whether there are traces of attacker login and attacks. The traces can also be used for source tracing analysis and forensics.

- The following slides describe how to check files, processes, and system information in Windows and Linux.
- Other emergency response technologies are as follows:
 - User analysis: View user login records to check whether unauthorized accounts used by attackers for backdoor login are added.
 - Network connection analysis: Check whether abnormal network connections exist. Some common backdoor connections have fixed port numbers. You can determine whether the system is attacked based on the network connections.

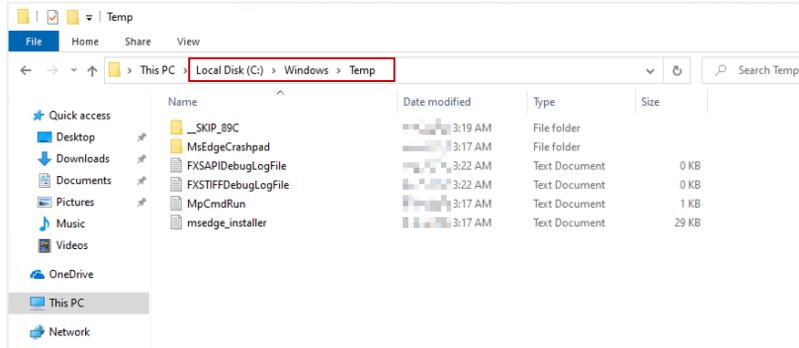
Checking Files (1/3)

- Check abnormal startup files: In the Windows operating system, choose **Start > Run > msconfig**. In the displayed window, check whether there are unknown abnormal startup items.



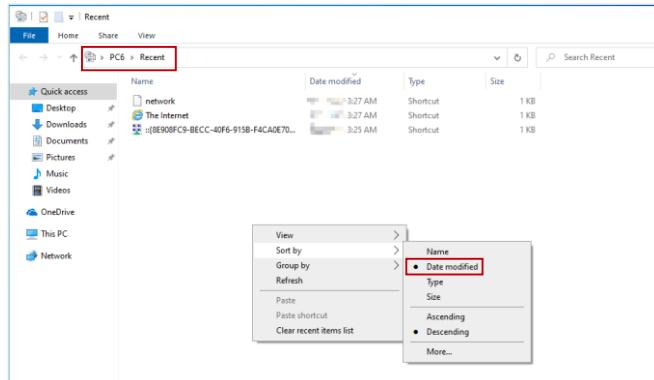
Checking Files (2/3)

- Check whether abnormal files (for example, .exe files) exist in the Temp (or tmp) directory (for example, C:\Windows\Temp) of each disk in the system. This directory usually stores temporary files generated by the Windows system and may be used by attackers.



Checking Files (3/3)

- Check the recently used files in the system. Choose **Start > Run > %UserProfile%\Recent**, open the **Recent** folder, sort the files by modification date, and check whether the recently modified files contain unknown abnormal files.



- In this step, you can right-click a file to view the creation time, modification time, and access time of the file. Generally, hackers change the modification time of the file to bypass the detection. If the modification time is earlier than the creation time, the file is suspicious.
- You can also check whether some system files are modified, for example, .dll files (generally in the system directory).

Checking Processes (1/3)

- Common Trojan horses, viruses, and malicious codes are spread over the network to infect a large number of terminals on a LAN. Determine whether some ports commonly used by viruses exist through checking processes.
- During process check, you can use the network connection analysis tool **netstat** provided by the system to analyze the network connection. Details about the **netstat** command:

```
netstat -{a,n,o,r,s}
    -a      Display information about all network connections, routing tables, and network interfaces.
    -n      Display the address and port number in numeric format.
    -o      Display the ID of the process related to each connection.
    -r      Display the IP routing table.
    -s      Display protocol-based statistics, default location, and IP address.
```

Checking Processes (2/3)

- An example of the **netstat** command output is as follows:

Active Connections				
Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	900
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING	1028
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING	5516
TCP	0.0.0.0:8900	0.0.0.0:0	LISTENING	2848
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING	680
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING	524
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING	1204
TCP	127.0.0.1:8900	127.0.0.1:49669	ESTABLISHED	2848
TCP	127.0.0.1:8900	127.0.0.1:49672	ESTABLISHED	2848
TCP	127.0.0.1:8900	127.0.0.1:49673	ESTABLISHED	2848

- PID indicates the process ID.
- The states in the output of the **netstat** command:
 - LISTENING**: indicates the listening state.
 - ESTABLISHED**: indicates the connection is set up.
 - CLOSE_WAIT**: indicates that the peer end proactively closes the connection or the connection is interrupted due to a network exception.

Checking Processes (3/3)

- After detecting an abnormal connection based on the port number, run the **tasklist** command to locate the process name.

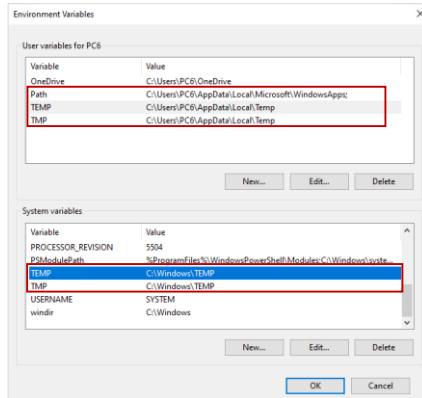
```
C:\Users\PC1> tasklist | findstr 3816 → PID  
spoolsv.exe 3816 Services 0 17,452 K
```

- Run the **wmic process** command to obtain the full path information of the process.

```
C:\Users\PC1> wmic process | findstr spoolsv.exe → Process name  
spoolsv.exe  
Win32_Process 20211028123614.065414+480  
Win32_ComputerSystem DESKTOP-DUOAB0V spoolsv.exe  
3816 702 157812500  
spoolsv.exe Win32_OperatingSystem Microsoft Windows 10 ???|C:\Windows\Device\Harddisk0\Partition3  
141847 1823255 566354 9500 640 12404 2203474538496 27668  
8 9728000 3816 29 209 34 225 31270  
11761418 0 7 97500000 2203462455296 10.0.19042 17870848 138386  
7831604
```

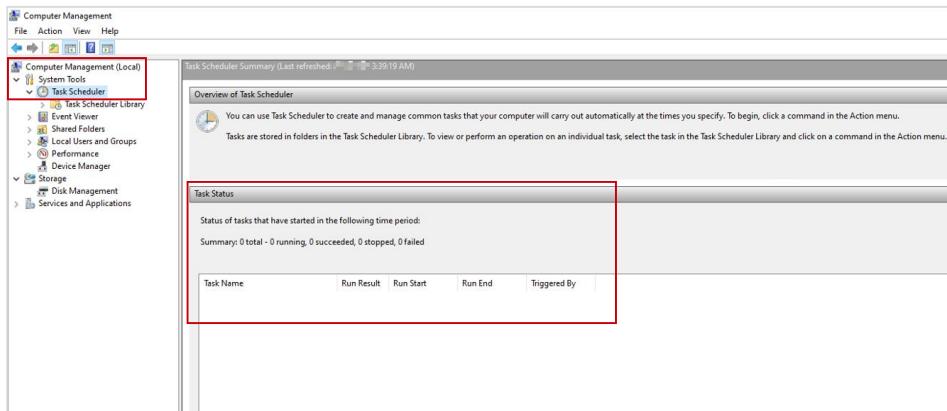
Checking System Information (1/3)

- Check whether the environment variables (system variables and user variables) of the Windows operating system are normal. For example, check whether the value of the system variable **TEMP** or **TMP** is **C:\Windows\TEMP** and whether other invalid paths are added to the user variable **Path**.



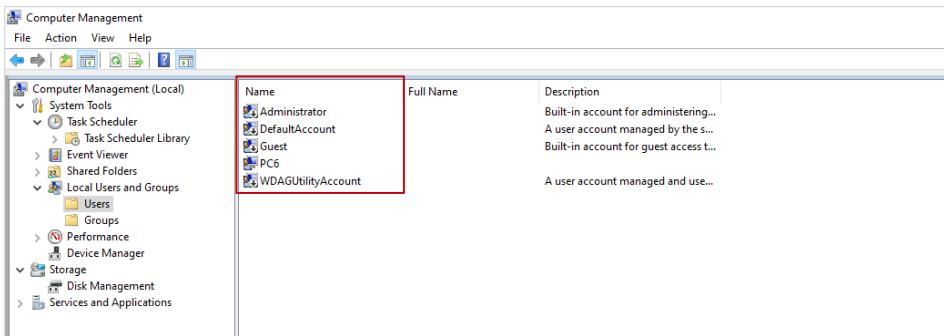
Checking System Information (2/3)

- Right-click **This PC**, and choose **Manage > System Tools > Task Scheduler** to check whether any task schedule program that is not created by the user exists.



Checking System Information (3/3)

- Right-click **This PC**, and choose **Management** > **System Tools** > **Local Users and Groups** to check whether undisclosed accounts exist. The user whose name ends with \$ is an undisclosed account.



- In addition, you can run the commands in the CLI to query the user information. For example, you can run the **query user** command to view the session connections of the current login user to determine whether someone is remotely logging in to the terminal.

Checking Files (1/5)

- Run the **ls** command to check whether abnormal files, such as .sh files, exist in the **/tmp**, **/usr/bin**, and **/usr/sbin** directories.

```
[root@iMaster-NCE ~]# ls -alt /tmp/
total 116
drwx----- 2 omm      wheel    4096  17:13 hsperfdata_omm
drwxrwxrwx. 11 root     root     20480 17:13 .
drwx----- 2 ommdba   wheel    4096  17:13 hsperfdata_ommdba
-rw------- 1 omm      wheel    3002  17:13 report.json
-rwxrwxrwx  2 sysus   sysus    23570 17:13 sysauto.sh      //Focus on the executable script files.
-rw-r--r--  1 root     root     30044 17:13 cronlock.log
drwxr-x---  2 omm      wheel    4096  17:12 omm
drwxr-x---  2 ossadm   ossgroup 4096  17:08 hsperfdata_ossadm
drwxr-x---  2 ossuser  ossgroup 4096  16:31 hsperfdata_ossuser
```

Checking Files (2/5)

- Check whether abnormal programs are added to the startup items.

```
[root@iMaster-NCE ~]# ls -alt /etc/init.d/      //This directory stores the startup item file.  
total 52  
drwxr-xr-x. 10 root root 4096 12:58 ..  
drwxr-xr-x.  2 root root 4096 20:28 .  
-rwxr-x---.  1 root root 658   20:28 ossipmc01  
-rw-r-----.  1 root root 46    20:20 boot.local  
-rw-r--r--.  1 root root 18325 20:21 functions  
-rwxr-xr-x.  1 root root 9363  20:21 network  
-rw-r--r--.  1 root root 1161  20:21 README
```

Checking Files (3/5)

- View files in a specific directory by time to check whether any file is maliciously modified. For example, view key system directories such as **/bin**, **/sbin**, **/usr/bin**, and **/usr/sbin**.

```
[root@iMaster-NCE sbin]# ls -alt | head -n 10      //Only the first 10 lines are displayed.  
total 50768  
dr-xr-xr-x. 2 root root 20480 12:04 .  
lrwxrwxrwx. 1 root root 26 12:47 ebtables -> /etc/alternatives/ebtables  
lrwxrwxrwx. 1 root root 24 12:47 ifdown -> /etc/alternatives/ifdown  
lrwxrwxrwx. 1 root root 22 12:47 ifup -> /etc/alternatives/ifup  
lrwxrwxrwx. 1 root root 27 12:47 ip6tables -> /etc/alternatives/ip6tables  
lrwxrwxrwx. 1 root root 35 12:47 ip6tables-restore -> /etc/alternatives/ip6tables-restore  
lrwxrwxrwx. 1 root root 32 12:47 ip6tables-save -> /etc/alternatives/ip6tables-save  
lrwxrwxrwx. 1 root root 26 12:47 iptables -> /etc/alternatives/iptables  
lrwxrwxrwx. 1 root root 34 12:47 iptables-restore -> /etc/alternatives/iptables-restore
```

Checking Files (4/5)

- Check the historical command record file of a user. In the Linux operating system, the commands executed by a user are saved in the **.bash_history** file in the home directory of the user. You can view the file to check whether the user has executed abnormal commands.

```
root@kali: ~# cat /root/.bash_history |more
ifconfig
ping 192.168.250.30
ping 192.168.253.130
service networking restart
ifconfig
ping www.baidu.com
/etc/init.d/networking restart
ifconfig
ping www.baidu.com
/etc/init.d/network-manager restart
ifconfig
ping www.baidu.com
ping 192.168.253.130
/etc/init.d/networking restart
ping www.baidu.com
vim /etc/network/interfaces
ifconfig
ping 172.24.125.77
/etc/init.d/networking restart
ifconfig
ping 172.24.125.77
rdesktop -u -p 172.24.125.77:3389
rdesktop -u -p 172.24.125.77
```

Checking Files (5/5)

- All user names in the Linux operating system are stored in the **/etc/passwd** file. You can check this file to determine whether unauthorized user names exist. You can also view the login permission of a user in this file. For example, **/sbin/nologin** indicates that the user cannot log in.

```
[sopuser@iMaster-NCE ~]$ cat /etc/passwd
root:x:0:root:/root:/bin/bash
bin:x:1:bin:/bin:/sbin/nologin
daemon:x:2:daemon:/sbin:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
ftpuser:x:4001:2000:/opt/backup/ftpboot:/usr/libexec/openssh/sftp-server
sopuser:x:3008:2000:/home/sopuser:/bin/bash
dbuser:x:3002:1999:/home/dbuser:/bin/bash
tcpdump:x:72:72:::/sbin/nologin
```

The first column
indicates the user names.

The last column indicates
the user login permissions.

- If an abnormal user is found and the last column is **nologin**, you can continue to check the historical commands executed by the user. Determine whether abnormal commands are executed by checking the **.bash_history** file about the user.

Checking Processes (1/3)

- You can run the **top** command to dynamically view the overall running status of the system in real time and check whether abnormal processes occupy a large number of CPU and memory resources.

```
top-18:24:39 up 56 days, 21:59,  1 user, loadaverage: 29.33, 27.29, 27.78
Tasks: 1094 total,   6 running, 1086 sleeping,   0 stopped,   2 zombie
%Cpu(s): 41.3us, 12.8sy,  0.0ni, 44.6id,  0.0wa,  0.8hi,  0.5si,  0.0st
MiB Mem: 257185.4 total,   6202.1 free, 98947.1 used, 152036.2 buff/cache
MiB Swap:     0.0 total,     0.0 free,     0.0 used. 145111.7 avail Mem

      PID  USER      PR  NI    VIRT      RES      SHR      S  %CPU  %MEM     TIME+ COMMAND
190837  omm      20   0  35.7g  492048  45900  S 220.9  0.2   0:06.76  java
15062  ossuser   20   0  17.5g   1.4g  18912  S 220.6  0.6  65690:23  java
117849  omm      20   0 8510652 900868  77220  S 113.4  0.3  84099:47  java
182155  dbuser   20   0 2136612  1.2g  15848  S 102.9  0.5  22028:32  zengine
221290  ossuser   20   0 9917328  3.9g  32708  S  33.3  1.6  26992:00  java
  55004  ossadm   20   0  885908  95656  12940  S  18.0  0.0  14357:43  python
182557  dbuser   20   0 3236032  1.9g  16092  S  14.1  0.8  4739:08  zengine
```

- The displayed CPU usage is the usage sum of all cores. If an application uses 30% CPU resources on all four cores, the CPU usage exceeds 100%.
- The parameters in the **top** command output are described as follows:
 - PID: indicates the process ID.
 - USER: indicates the user.
 - PR: indicates the priority.
 - NI: indicates the nice value. A negative value indicates a high priority and a positive value indicates a low priority.
 - SHR: indicates the size of the shared memory, in KB.
 - S: indicates the process status. S in the S column indicates sleep.
 - %CPU: indicates the CPU usage.
 - %MEM: indicates the percentage of the physical memory occupied by a process.
 - TIME+: indicates the total CPU time used by the process, in 1/100 seconds.
 - COMMAND: indicates the command name or command line.

Checking Processes (2/3)

- Run the **netstat** command to check the network connection and check whether suspicious listening ports exist.

```
[root@iMaster-NCE ~]# netstat -antlp | more
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State      PID/Program name
tcp        0      0 192.168.10.103:22885    0.0.0.0.*        LISTEN     143720/java
tcp        0      0 192.168.10.103:22853    0.0.0.0.*        LISTEN     97346/java
tcp        0      0 127.0.0.1:25925       0.0.0.0.*        LISTEN     150759/java
tcp        0      0 192.168.10.103:27333    0.0.0.0.*        LISTEN     76275/traffic_manag
tcp        0      0 192.168.10.103:26533    0.0.0.0.*        LISTEN     186711/redis-server
tcp        0      0 192.168.10.103:26661    0.0.0.0.*        LISTEN     186090/redis-server
tcp        0      0 192.168.10.103:21093    0.0.0.0.*        LISTEN     117849/java
tcp        0      0 127.0.0.1:22501       0.0.0.0.*        LISTEN     65649/java
tcp        0      0 127.0.0.1:20006       0.0.0.0.*        LISTEN     101554/java
```

- The parameters in the **netstat** command are described as follows:
 - a: displays sockets in all connections.
 - n: uses the IP address instead of the domain name server.
 - t: displays the TCP connection status.
 - u: displays the UDP connection status.
 - v: displays the command execution process.
 - p: displays the identifier and name of the program that is using the socket.
 - s: displays the statistics table of network working information.
- Recv-Q** and **Send-Q** indicate the receiving queue and sending queue, respectively.

Checking Processes (3/3)

- If an abnormal process is discovered in the output of the **top** or **netstat** command, run the **ps** command to view the detailed information about the process. You can use the pipe character | and the command **grep** to check information about a specified process.

```
[root@iMaster-NCE ~]# ps -aux | grep 166878
dbuser 166878 0.0 0.0 253532 5372 ? Ssl Apr14 77:36 /opt/redis/bin/redis-server 192.168.10.103:26532
root 241285 0.0 0.0 213136 828 pts/2 S+ 21:09 0:00 grep --color=auto 166878
```

Process
ID

- The parameters in the **ps** command are described as follows:
 - a: displays the processes of all users.
 - u: displays the user name or user ID.
 - x: displays all processes without distinguishing them by terminals.

Checking System Information (1/2)

- Run the **crontab** command to check whether abnormal scheduled tasks exist.

```
[root@iMaster-NCE ~]# crontab -l  
0 */2 * * * /bin/bash /etc/timing_task.sh      //Scheduled task
```

- View the **/etc/rc.local** file to check whether abnormal startup programs exist.

```
[root@iMaster-NCE ~]# cat /etc/rc.local      //The rc.local file is automatically executed upon system startup.  
touch /var/lock/subsys/local  
systemctl stop ntpd  
ntpdate 192.168.10.103 >>/var/log/NCE/logs/time_sync.log  
hwclock  
systemctl start ntpd  
iptables -A INPUT -p icmp --icmp-type timestamp-request -j DROP  
iptables -A OUTPUT -p icmp --icmp-type timestamp-reply -j DROPD
```

Checking System Information (2/2)

- Check the last login time of all users in the system and check whether abnormal user logins occur recently.

```
[root@iMaster-NCE ~]# lastlog
Username      Port    From          Latest
root          pts/2   Fri Jun10 21:03:02 +0800 XXXX //XXXX indicates the year.
bin           bin     **Never logged in**
daemon        daemon  **Never logged in**
adm           adm    **Never logged in**
```

- View the **\$PATH** environment variable to check whether invalid or risky paths exist.

```
[root@iMaster-NCE ~]# echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/root/bin
```

Log Analysis

- Logs are generated during the running of devices and systems, recording information about normal events and exceptions. By viewing logs, engineers can learn about the overall running status of devices and service systems in a certain period of time. In addition, engineers can perform source tracing and evidence collection after a security incident occurs.

Log record

- Logs record a large amount of information generated during the running of computer software and hardware. Logs can be used for problem analysis, service statistics, and decision-making.

Fault locating

- Logs help engineers quickly locate fault causes, improving O&M efficiency.

Fault analysis

- After the fault is rectified, you can view the logs of the entire process to analyze the root cause of the fault and provide reference for subsequent optimization.

Attack source tracing

- Network attacks usually have traces. By viewing logs, you can find the attack source and attack mode.

- For a security device, system logs record various attack events, including the attack source IP addresses, attack characteristics, and whether the attacks are blocked.
- For an OS, system logs record the overall system information, user login or authorization information, and security incident information.
- For a service system, service logs record various access behaviors of users. For example, the service logs of an Nginx server record the IP address, request type, and request time of guests. The service logs can be used for fault locating and attack backtracking.

Log Format — Network Devices

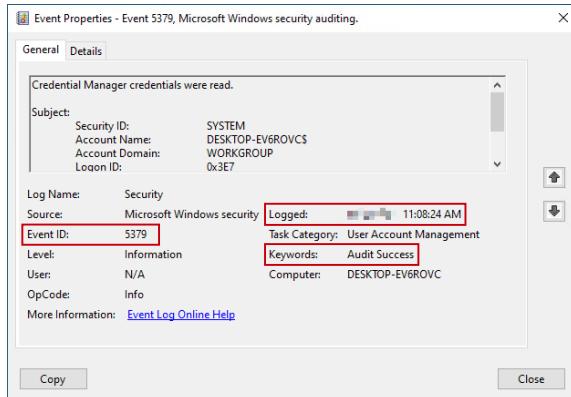
- System logs of network devices, such as routers, switches, and firewalls, are stored in syslog format and can be easily read.
- Log format description:
 - Jul XX XXXX 15:55:06: indicates the timestamp, showing the time when the log is generated.
 - SW4-S57: indicates the name of the device that generates the log.
 - %%01: indicates the vendor flag. %% is a fixed field, and 01 indicates a specific vendor.
 - IFNET: indicates the name of the service module to which the log belongs.
 - 4: indicates the log level. The value ranges from 0 to 7. A smaller value indicates a higher severity.
 - IF_ENABLE(l)[68]: indicates the summary of the log.
 - Interface GigabitEthernet0/0/1 has been available: log content.

```
Jul XX XXXX 15:55:06 SW4-S57 %%01 IFNET/4/IF_ENABLE(l)[68]:Interface GigabitEthernet0/0/1 has been available.
```

- In addition to the syslog format, logs of traditional communications devices and security devices can also be in binary, dataflow, or netflow format. These formats are designed to facilitate computer processing and data transmission but are not suitable for engineers to read. Therefore, it is more common to use syslogs for attack source tracing.

Log Format — Windows

- You can view Windows logs in the Event Viewer of a Windows host. Common logs include system logs, security logs, setting logs, and application logs.



38 Huawei Confidential

 HUAWEI

- You can view the following information in Windows logs: log name, log source, event ID, level, user, and log generation time (**Logged**).
- To facilitate log processing and analysis, you can save Windows logs as a text file, and open the file using a text editor to search for logs based on a specific source IP address.

Log Format — Linux

- In Linux, different types of logs are stored in different directories. The following table lists the common log types in Linux.

Log Type	Description
/var/log/messages	Records the overall system information.
/var/log/auth.log	Records system authorization information, including information about user login and permission mechanism.
/var/log/userlog	Records information about users of all levels.
/var/log/cron	Records the execution of the crontab command.
/var/log/vsftpd.log	Records logs related to the Linux FTP application.
/var/log/lastlog	Records the latest login information of users. You can run the lastlog command to view the log information.
/var/log/secure	Records the user names and passwords entered in most applications and whether the login is successful.
/var/log/wtmp or /var/log/utmp	Records information about accounts that successfully log in to the system.
/var/log/faillog	Records information about accounts that fail to log in to the system.

- A log example of a Linux server is as follows:

```
Jun XX XXXX 18:22:35 iMaster-NCE sudo[260687]:    omm : TTY=unknown ; PWD=/opt/huawei/Bigdata/om-server_8.0.2.1/OMS/workspace0/ha/module/harm/plugin/script ; USER=root ;
COMMAND=/var/lib/sudo/Bigdata/sudo/runtime/sudoExecute.sh m_arping bond0 192.168.10.103
```

Source Tracing and Forensics Based on Logs (1/2)

OS logs

/var/log/secure log in Linux:

```
[root@iMaster-NCE log]# tail -n 10 secure
Jun 16 10:19:17 iMaster-NCE su[188909]: pam_unix(su-l:session):
session opened for user ommdba by (uid=0)
Jun 16 10:19:17 iMaster-NCE su[188909]: pam_unix(su-l:session):
session closed for user ommdba
Jun 16 10:19:17 iMaster-NCE su[188950]: pam_unix(su-l:session):
session opened for user omm by (uid=0)
Jun 16 10:19:17 iMaster-NCE su[188950]: pam_unix(su-l:session):
session closed for user omm
```

- **/var/log/secure** contains authentication and authorization information. By viewing this log, you can check whether any user attempts to log in to the host using brute force cracking.
- Based on OS logs, you can analyze whether unauthorized users have logged in to the system, and determine whether the system has been intruded or whether backdoor accounts have been left.

Service system logs

access.log of the Nginx application:

```
192.168.10.103 - - [XX/Apr/XXXX:09:14:15 +0800] "GET
/campusLogin/images/logo_huawei.ico?v=1649983171392 HTTP/1.1"
200 1150
"https://10.154.176.119:8447/unisso/login.action?service=%2Funi
sess%2Fv1%2Fauth%3Fservice%3D%252FcampusNCE%252Fcampus
NCEIndex.html" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.88
Safari/537.36"
"192.168.10.200" - 0.000 -
```

- The **access.log** file records user access information, including the guest IP address, access time, HTTP request method and URL, and client type.
- Service system logs (such as Apache and Nginx logs) can be used to determine whether attack behaviors (such as injection attacks and script execution) exist.

Source Tracing and Forensics Based on Logs (2/2)

Security device logs

Syslogs on an IPS device:

```
Jun XX XXXX 11:12:13 FW3 %%01IPS/4/DETECT(l)[0]:An intrusion was detected. (SyslogId=1, VSys="public", Policy="pass", SrcIp=100.100.1.10, DstIp=10.3.0.100, SrcPort=55411, DstPort=80, SrcZone=trust, DstZone=trust, User="unknown", Protocol=TCP, Application="HTTP", Profile="icmp", SignName="SQL Injection Attack - Bool-Based Blind Injection", SigId=6159300, EventNum=1, Target=server, Severity=medium, Os=all, Category=Injection, Reference=NA, Action=Block)
```

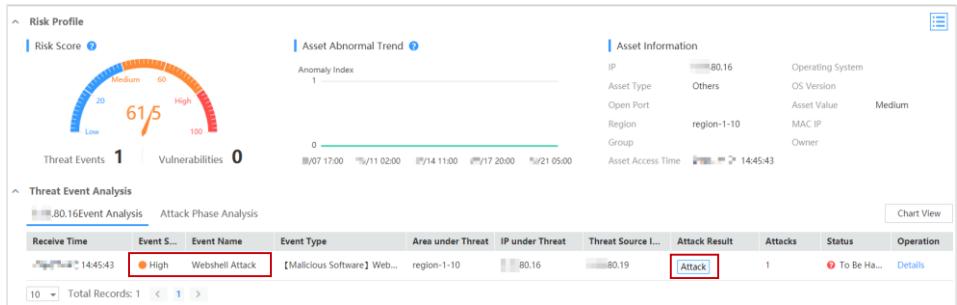
- IPS logs record the source and destination IP addresses, protocol numbers, source and destination port numbers, application types, and matched signatures of attacks.
- By viewing security device logs, you can determine whether the information system is intruded and work out effective measures to defend against attacks. In addition, source tracing and forensics can be performed based on log information.

Contents

1. Emergency Response Overview
2. Emergency Response Process
3. **Emergency Response Technologies and Cases**
 - Emergency Response Technologies
 - Emergency Response Cases

WannaCry Case — Identification Phase (1/2)

- When an organization is attacked by WannaCry, emergency response personnel can learn about the attack from the alarm information in the Huawei HiSec Insight security situational awareness system or from the feedback of employees in the organization.
- As shown in the following figure, HiSec Insight shows that high-risk virus attacks have successfully broken the defense line. Emergency response personnel need to rate and report security incidents in a timely manner. If an emergency response plan is available, start the plan. If no emergency response plan is available, take measures in compliance with the emergency response process.



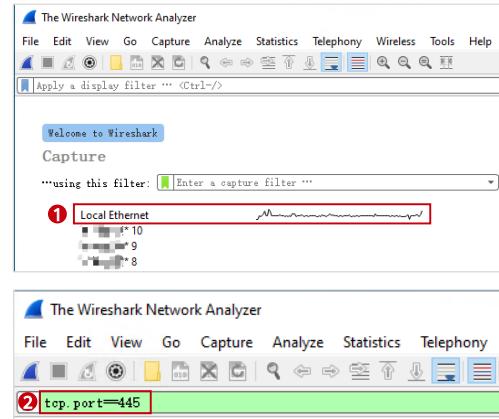
43 Huawei Confidential

HUAWEI

- For small-, medium-, and large-sized enterprises, Huawei launches the big data-based APT defense product HiSec Insight (HiSec Insight for short). HiSec Insight can effectively collect massive basic network data, such as network traffic and network or security logs of various devices. Based on real-time and offline big data analytics, machine learning technologies, expert reputation database, and information retrieval, HiSec Insight effectively detects potential threats and APTs on the network as well as the network-wide security situation of the enterprise intranet.

WannaCry Case — Identification Phase (2/2)

- Comprehensively check for virus infection on the network:
 - IPS detection: Mirror traffic to the IPS device and configure detection policies.
 - Packet obtaining and analysis: Obtain packets through Wireshark, and analyze network traffic.
 - Use other dedicated detection tools.
- Steps of the packet obtaining and analysis at the network layer:
 - Connect the PC to be detected to the network and enable port 445.
 - Use Wireshark to monitor the local network.
 - Set the traffic filtering rule **tcp.port==445** and obtain the traffic.
 - Check whether the traffic is normal.



WannaCry Case — Containment Phase (1/5)

- After detecting a virus attack, the spread of the virus needs to be immediately contained. Generally, the following measures are taken:
 - Isolate known infected hosts and prevent them from accessing the network.
 - Isolate the network and block port 445 on devices such as firewalls and routers to prevent worms from spreading between networks.

Disabling the Server Message Block (SMB) protocol on the firewall

The screenshot shows a configuration page for a firewall or router. Under the 'Source and Destination' section, the 'Service' field contains 'smb' with a red box around it. Below this, under 'Action', the 'Deny' radio button is selected with a red box around it. Other fields like 'Source Zone', 'Destination Zone', and 'VLAN ID' are also visible.

Blocking the TCP port 445 on the router

```
<Huawei> system-view  
[Huawei] acl number 3001  
[Huawei-acl-3001] rule deny tcp destination-port eq 445  
[Huawei-acl-3001] rule permit ip
```

Note: This ACL needs to be applied to the corresponding interface on the router.



WannaCry Case — Containment Phase (2/5)

- Send internal notifications through offline meetings, instant messaging software, SMS messages, and emails, and organize employees to take emergency response measures.
 - Isolate the infected host. If the host is connected to a wired network, remove the network cable. If the host is connected to a wireless network, disconnect the wireless network.
 - Employees check whether their office PCs are infected with viruses. Check whether there are **.wncry** files and whether a ransomware page is displayed.
 - If a PC is infected with viruses, report the virus immediately and ask professional cyber security engineers to handle the virus.
 - If the PC is not infected with viruses, you are advised to harden the system immediately.

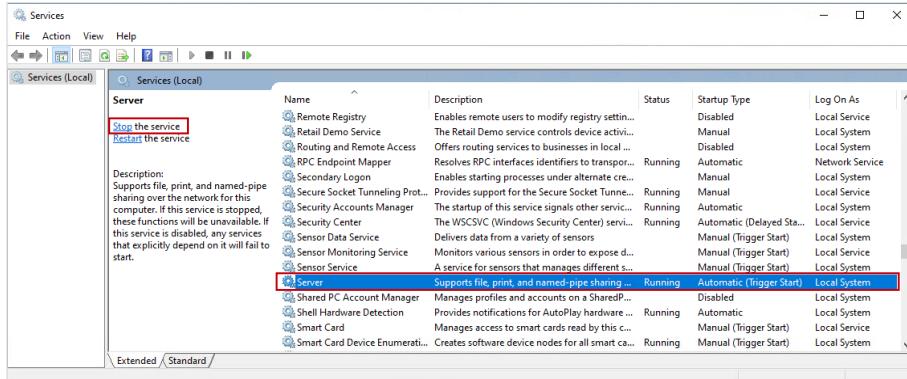
WannaCry Case — Containment Phase (3/5)

- Security hardening for Windows hosts that are not infected with viruses: Configure firewall policies to block TCP port 445.

The screenshot shows two windows side-by-side. The left window is the 'New Inbound Rule Wizard' - 'Rule Type' step. It lists five steps: Rule Type (selected), Protocol and Ports, Action, Profile, and Name. Step 1 is highlighted with a red box and the number 1. The 'What type of rule would you like to create?' section contains three options: Program (radio button not selected), Port (radio button selected, highlighted with a red box and the number 2), and Predefined (radio button not selected). The right window is the 'Action' step of the wizard. It lists five steps: Rule Type, Protocol and Ports, Action (selected), Profile, and Name. Step 5 is highlighted with a red box and the number 5. It asks 'Does this rule apply to TCP or UDP?' with options TCP (selected, highlighted with a red box and the number 3) and UDP. Below that, it asks 'Does this rule apply to all local ports or specific local ports?' with options All local ports (radio button not selected) and Specific local ports (radio button selected, highlighted with a red box and the number 4). A text input field shows '445' with the placeholder 'Example: 80, 443, 5000-5010'. The right window also includes sections for 'Allow the connection' (radio button not selected) and 'Allow the connection if it is secure' (radio button not selected). The bottom right of the right window features the HUAWEI logo.

WannaCry Case — Containment Phase (4/5)

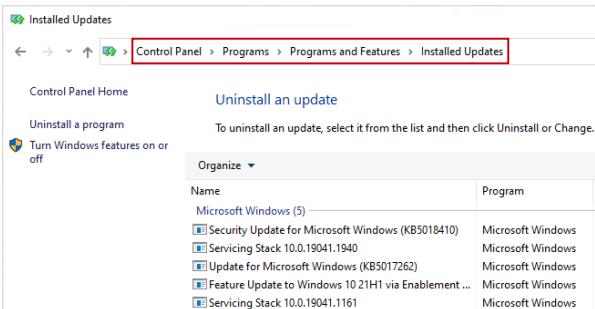
- Security hardening for Windows hosts that are not infected with viruses: Disable the file sharing and printing services.



WannaCry Case — Containment Phase (5/5)

- Security hardening for Windows hosts that are not infected with viruses:
 - System upgrade: Windows 2003, 2008, and XP have stopped the security patch service and need to be upgraded to the latest version.
 - Patch repair: Install the dedicated patch released by Microsoft. The patch ID varies according to the system version.

System Version	Patch ID
Windows 7 Windows Server 2008 R2	KB4012212
	KB4012215
Windows Server 2012	KB4012214
	KB4012217
Windows Server 2012 R2	KB4012213
	KB4012216
Windows 10	KB4012606



The screenshot shows the Windows Control Panel's 'Installed Updates' page. The navigation path 'Control Panel > Programs > Programs and Features > Installed Updates' is highlighted with a red box. Below the path, there are links for 'Control Panel Home', 'Uninstall an update', 'Uninstall a program', and 'Turn Windows features on or off'. A 'Organize' dropdown menu is open. The main area displays a table of installed updates with columns for 'Name' and 'Program'. The updates listed are:

Name	Program
Microsoft Windows (5) —	Microsoft Windows
Security Update for Microsoft Windows (KB5018410)	Microsoft Windows
Servicing Stack 10.0.19041.1940	Microsoft Windows
Update for Microsoft Windows (KB5017262)	Microsoft Windows
Feature Update to Windows 10.21H1 via Enablement ...	Microsoft Windows
Servicing Stack 10.0.19041.1161	Microsoft Windows

WannaCry Case — Eradication Phase

- Take the following measures on infected hosts:
 - Disconnect the network and isolate the infected hosts.
 - Determine the importance of the encrypted files.
 - If the encrypted files are unimportant or the files have been backed up, perform low-level formatting on the disk and reinstall the system.
 - If the files are important and are not backed up, wait for the decryption progress.

- In this case, it is not recommended to pay ransom for encrypted files.

WannaCry Case — Recovery Phase

- For hosts that have important encrypted files, try to restore the files.
- For networks:
 - Add WannaCry to the virus signature database of the security device and set antivirus policies to block virus intrusion and spread.
 - For the network that requires the file sharing or printing service, enable port 445 on some hosts first, and then all hosts based on the site requirements.
 - Continuously monitor network traffic and check whether a host is infected again.
 - Deliver the latest system patches in a unified manner to harden hosts.

WannaCry Case — Lessons Learned Phase

- Summarize the emergency response process and measures, and record problems and solutions.
- Improve the security awareness of all employees, and popularize the damages, common transmission methods, and preventive measures of viruses.
- Periodically detect network vulnerabilities, pay attention to the latest patch release, and fix patches in a timely manner.

Quiz

1. (Single-answer question) After analyzing operating system logs and security device logs to determine the source IP address of the attacker, the administrator modifies the security device policy to block the source IP address. Which of the following emergency response phase does this operation belong to? ()
 - A. Identification
 - B. Containment
 - C. Eradication
 - D. Recovery

Summary

- This course describes the necessity and standard process of the emergency response, and common handling methods for security incidents. In addition, this course describes the technologies and cases related to the emergency response.
- After learning this course, you will be able to understand the objectives and handling methods in different emergency response phases, master common emergency response technologies, and improve the capability of coping with cyber attacks.

Recommendations

- Huawei official websites:
 - Enterprise service: <https://e.huawei.com/en/>
 - Technical support: <https://support.huawei.com/enterprise/en/index.html>
 - Online learning: <https://learning.huawei.com/en/>

Acronyms and Abbreviations

Acronym/Abbreviation	Full Name
IPS	Intrusion Prevention System
UDP	User Datagram Protocol
TCP	Transmission Control Protocol
PID	Process ID

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。
Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

Copyright©2022 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product performance, market position, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.



Network Access Control



Foreword

- With the application and development of the network, more and more important information is transmitted and stored through the network. Against this backdrop, cyber crimes in various forms increase sharply. Security is not considered at the initial stage of designing an open and free network. Therefore, firewalls are deployed at the network border to defend against attacks from external networks. However, research shows that 80% of cyber security vulnerabilities exist inside the network. Faults caused by these vulnerabilities may cause serious damage to the network, including service system breakdown and network breakdown.
- Identity authentication is the first line of defense to ensure cyber security. Through identity authentication, users are granted corresponding access permissions. Internal network security can be greatly ensured through continuous authentication based on the never-trust rule and always granting minimal access permissions to users.
- This course introduces the network access control (NAC) technology, which helps you understand how to ensure the security of the internal network through combining access and authentication technologies.

Objectives

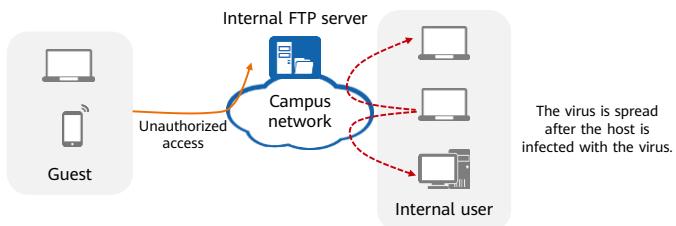
- On completion of this course, you will be able to:
 - Describe the basic concepts of NAC.
 - Describe the working principles of user identity authentication.
 - Describe common access authentication modes and their working principles.
 - Configure user access authentication.

Contents

- 1. Overview of NAC**
2. User Identity Authentication
3. Access Authentication
4. NAC Configuration

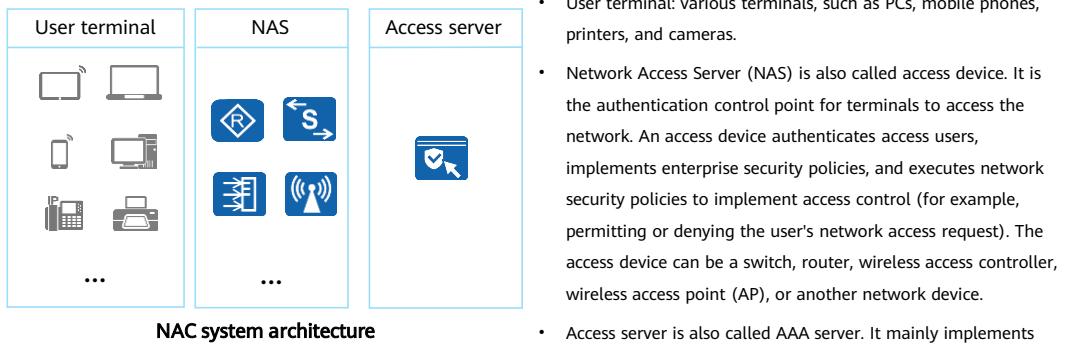
Technical Background of NAC

- Security risks of traditional enterprise network access:
 - Unauthorized users can access the campus network randomly, compromising campus information security.
 - A lack of permission control and access restrictions, increasing enterprise risks.
 - There are various types of terminals that access the campus network, and user behaviors on the campus network are difficult to manage and control. As user behaviors are not recorded, source tracing of security events cannot be performed.
- To ensure security, the campus network cannot grant access permissions to all terminals. Instead, it needs to authenticate the end users. Terminals that do not meet the conditions cannot access the network. In addition, user permissions are restricted and users' network access behaviors are recorded.



Overview of NAC (1/2)

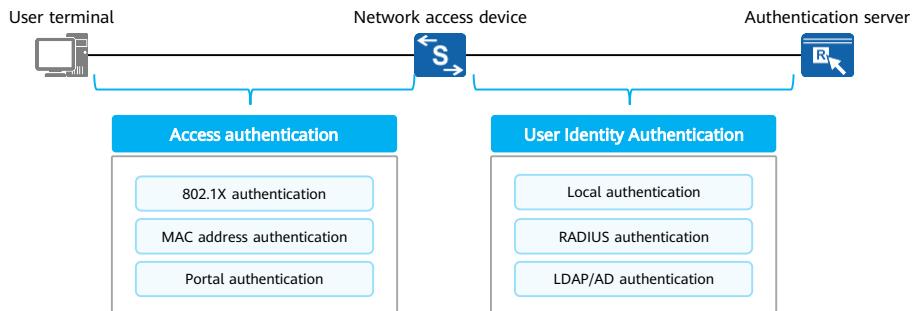
- NAC is an end-to-end security technology, which is used to ensure network security by authenticating clients and users who access a network.



- Generally, a terminal agent (or client software) is installed on a user terminal. It interworks with the access server to authenticate users, check terminal security, repair and upgrade the system, and monitor and audit terminal behaviors.
- The network access device can be a network device such as a switch, router, or AP. It has the following functions:
 - User identity authentication.
 - In various common authentication modes (such as 802.1X, MAC address, and Portal authentication), the network access device assists the client software and access server in authentication.
 - User permission control.

Overview of NAC (2/2)

- The entire process of network access of a user can be divided into two parts: access authentication and user identity authentication. Access authentication is performed between a user terminal and an access device, and user identity authentication is performed between an access device and an authentication server.
- Common access authentication modes include 802.1X authentication, MAC address authentication, and Portal authentication. Common user identity authentication modes include RADIUS authentication, LDAP/AD authentication, and local authentication.

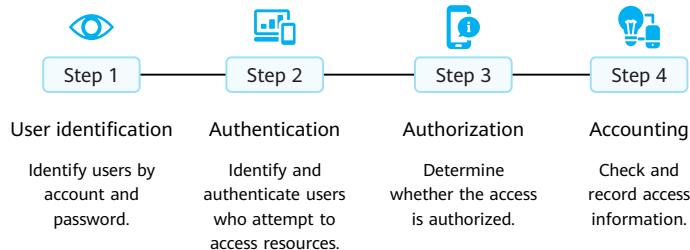


Contents

1. Overview of NAC
- 2. User Identity Authentication**
3. Access Authentication
4. NAC Configuration

Overview of AAA

- Authentication, authorization, and accounting (AAA) provides a management mechanism for network security.
 - Authentication: determines which users can access the network.
 - Authorization: authorizes users to use particular services.
 - Accounting: records the network resources used by users.



Common AAA Technical Solutions

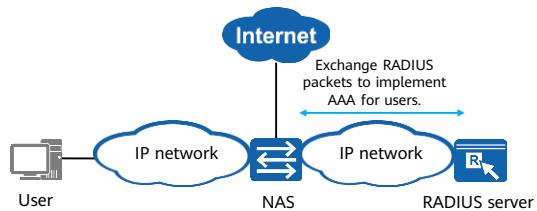
- Currently, Huawei devices support AAA based on RADIUS, HWTACACS, LDAP, and AD. RADIUS is most commonly used in actual applications.

Technical Solution	Interaction Protocol	Authentication	Authorization	Accounting
RADIUS	UDP	✓	✓	✓
HWTACACS	TCP	✓	✓	✓
LDAP	TCP	✓	✓	✗
AD	TCP	✓	✓	✗
Local authentication and authorization	/	✓	✓	✗

- In LDAP authentication, an LDAP client sends user passwords in cleartext to an LDAP server, which poses security risks. Kerberos provides a symmetrical key mechanism to improve password transmission security. Therefore, integrating the Kerberos protocol into LDAP authentication can prevent user password leakage during LDAP authentication. This authentication mode integrated with the Kerberos protocol is called AD authentication.

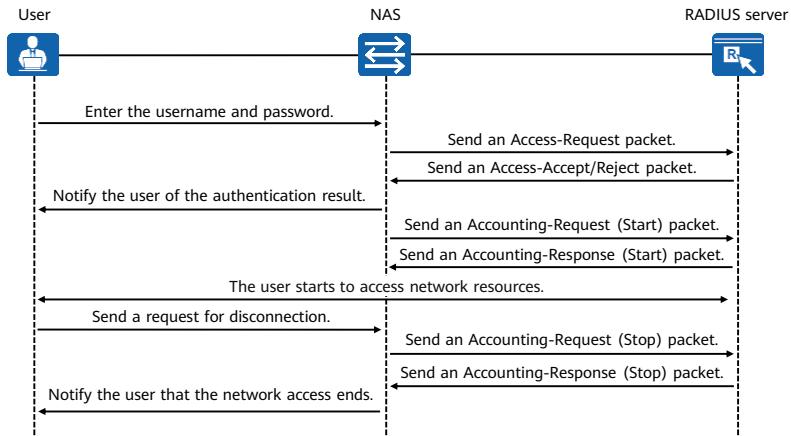
Overview of RADIUS

- AAA can be implemented using multiple protocols. RADIUS is most frequently used in actual scenarios.
- RADIUS is a distributed information exchange protocol using the client/server structure. It protects a network against unauthorized access and is often used on networks that require high security and allow remote user access.
- This protocol defines the User Datagram Protocol (UDP)-based RADIUS packet format and message transmission mechanism, and specifies UDP ports 1812 and 1813 as the authentication and accounting ports respectively.
- RADIUS has the following characteristics:
 - Client/Server model
 - Secure message exchange mechanism
 - Fine scalability



- RADIUS sometimes uses ports 1645 and 1646 as the default authentication port and accounting port respectively.
- RADIUS uses the typical client/server model. The access control device functions as the RADIUS client and the access authentication server for access users. The access control device transmits user information to the specified RADIUS server, and then performs corresponding operations (for example, permitting or denying the user's access request) based on the information returned from the server. The RADIUS server receives user connection requests, authenticates users, and returns all required information to the access control device.

RADIUS Authentication, Authorization, and Accounting Process



11 Huawei Confidential

HUAWEI

- The message exchange process between the RADIUS client and server is as follows:
 - If a user wants to access a network, the user needs to send a connection request containing the username and password to the RADIUS client (the access control device).
 - The RADIUS client sends an Access-Request packet containing the username and password to the RADIUS server.
 - If the request is valid, the RADIUS server completes authentication and sends the required authorization information to the RADIUS client. If the request is invalid, the RADIUS server sends the authorization failure information to the RADIUS client.
 - The RADIUS client notifies the user of whether the authentication is successful.
 - The RADIUS client permits or denies the user's access request according to the received authentication result. If the user access request is permitted, the RADIUS client sends an Accounting-Request (Start) packet to the RADIUS server.
 - The RADIUS server returns an Accounting-Response (Start) packet and starts accounting.
 - The user starts to access network resources.

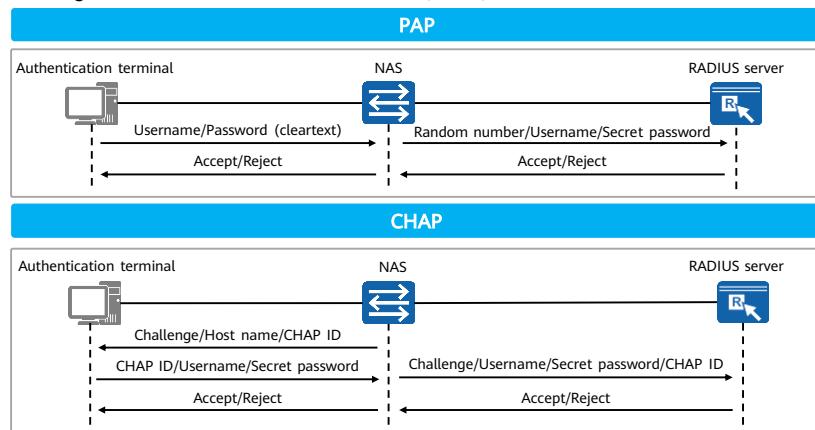
- When the user does not want to access network resources, the user sends a disconnection request to stop accessing network resources.
- The RADIUS client sends an Accounting-Request (Stop) packet to the RADIUS server.
- The RADIUS server returns an Accounting-Response (Stop) packet and stops accounting.
- The RADIUS client notifies the user that network access ends and the user stops accessing network resources.

RADIUS Packet

Packet Type	Description
Access-Request	<ul style="list-style-type: none">From the client to the server.The client sends user information to the server, and the server determines whether to permit the user's access request.
Access-Accept	<ul style="list-style-type: none">From the server to the client.If all attribute values in the Access-Request packet are acceptable (that is, the authentication succeeds), this packet is transmitted.
Access-Reject	<ul style="list-style-type: none">From the server to the client.If any attribute value in the Access-Request packet is unacceptable (that is, the authentication fails), this packet is transmitted.
Accounting-Request	<ul style="list-style-type: none">From the client to the server.The client sends user information to the server, requesting the server to start accounting.
Accounting-Response	<ul style="list-style-type: none">From the server to the client.The server notifies the client that the Accounting-Request packet has been received and accounting information has been correctly recorded.

RADIUS User Authentication Mode

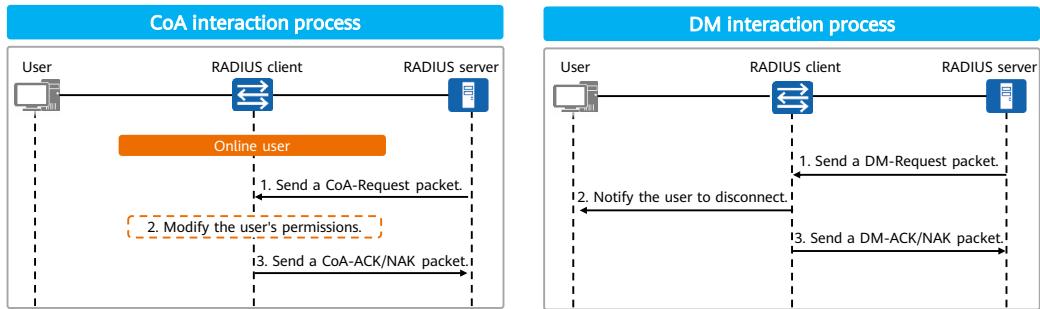
- RADIUS supports multiple user identity authentication modes, among which Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) are the most common ones.



- In PAP mode, the access control device carries the username and password (secret password, not cleartext password) through a RADIUS packet. The secret password (random number + key) is obtained by encrypting the cleartext password using the Message Digest Algorithm 5 (MD5). The random number is the authenticator field of the RADIUS packet, and the key value is the same key configured on both the RADIUS client and server.
- In CHAP mode, the access control device generates a 16-byte random code and sends it to the user together with an ID and the host name of the local device. After receiving the packet containing the preceding information, the authentication terminal uses its own device or software client to encrypt the CHAP ID and user password using the MD5 algorithm to generate a secret password. The secret password is sent to the access control device together with the username. The access control device uses the received username and secret password as the username and password, and sends the original 16-byte random code and CHAP ID to the RADIUS server. The RADIUS server searches the database based on the username and obtains the same key used by the authentication terminal for encryption. The RADIUS server uses the MD5 algorithm to encrypt the received CHAP ID, key, and 16-byte random code, and compares the result with the received password. If they match, the server returns an Access-Accept packet. Otherwise, the server returns an Access-Reject packet.
- Take 802.1X authentication as an example, if PAP is used, EAP packets exchanged between the authentication terminal and network access device carry information including the cleartext username and password. If CHAP is used, EAP packets exchanged between the authentication terminal and network access device carry information including CHAP ID, username, secret password, and Challenge.

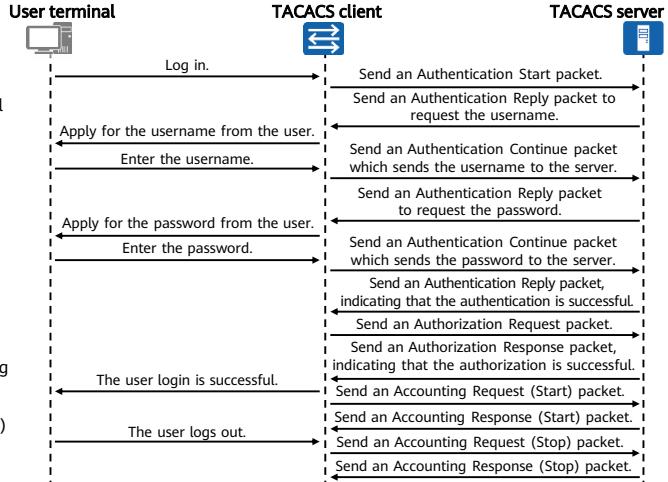
RADIUS Dynamic Authorization for Users

- The device supports the RADIUS Change of Authorization (CoA) and Disconnect Message (DM) functions. CoA provides a mechanism to dynamically change the permissions of online users, and DM provides a mechanism to disconnect users.
- CoA allows the administrator to modify the permissions of online users or reauthenticate the users through RADIUS after they are successfully authenticated.
- When a user needs to be disconnected, the RADIUS server sends a DM packet to the corresponding device.



Overview of HWTACACS

- Huawei Terminal Access Controller Access Control System (HWTACACS) is an enhanced security protocol based on TACACS (RFC 1492). It is a centralized information exchange protocol using the client/server architecture. It uses TCP for transmission and the TCP port number is 49.
- The authentication, authorization, and accounting services provided by HWTACACS are independent of each other and can be implemented on different servers.
- HWTACACS is used to perform authentication, authorization, and accounting for users accessing the Internet through Point-to-Point Protocol (PPP) or Virtual Private Dial-up Network (VPDN) and for administrators logging in to devices.



- HWTACACS and TACACS+ (supported by other vendors) support authentication, authorization, and accounting. The authentication process and implementation of HWTACACS are the same as those of TACACS+. HWTACACS is completely compatible with TACACS+.

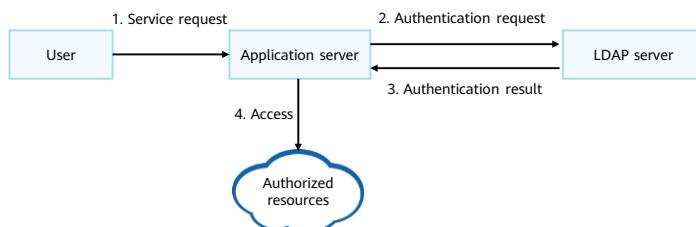
Comparison Between HWTACACS and RADIUS

Item	HWTACACS	RADIUS
Data transmission	Uses TCP, which is more reliable.	Uses UDP, which is more efficient.
Encryption mode	Shared key, encrypts the entire body of the packet except the standard HWTACACS header.	Shared key, encrypts only the password field in authentication packets.
Authentication and authorization	Separates authentication from authorization so that these services can be implemented on different security servers.	Combines authentication and authorization, which cannot be separated.
Command authorization	Supports authorization of configuration commands on devices.	Does not support authorization of configuration commands on devices.
Application scenario	Mainly used for device authentication due to the powerful command authorization function.	Widely applicable, including to both terminal authentication and device authentication.

- Both HWTACACS and RADIUS have the following characteristics:
 - Client/server structure
 - Shared key for encrypting the transmitted user information
 - Good flexibility and scalability

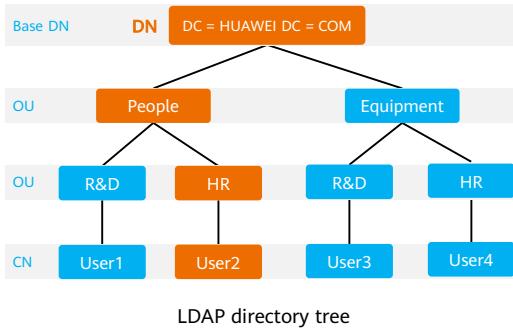
Overview of LDAP

- Lightweight Directory Access Protocol (LDAP) uses the client/server architecture.
- The LDAP server authenticates requests from the application server and specifies the range of resources available to users.
- LDAP defines multiple operations, for example, the bind and search operations for user authentication and authorization.



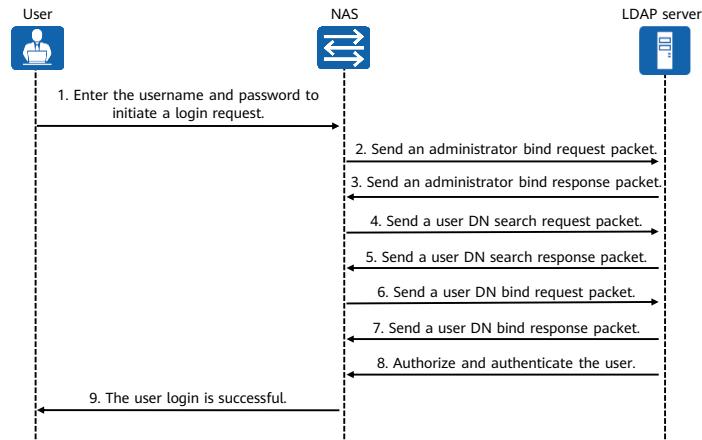
LDAP Directory

- A directory is a set of information with similar attributes that are organized in a logical and hierarchical manner. An LDAP directory is organized in a tree structure and consists of entries. An entry is made up of a collection of attributes that have a unique identifier called a Distinguished Name (DN). An attribute consists of the type and multiple values.



- Common Name (CN): indicates the name of an object.
- Domain Controller (DC): indicates the domain to which an object belongs. Generally, an LDAP server is a domain controller.
- DN: indicates the location of an object. It is described layer by layer from the object to the base DN. For example, the DN of User2 is "CN = User2, OU = HR, OU = People, DC = HUAWEI, DC = COM".
- Base DN: indicates the base DN.
- Organization Unit (OU): indicates the organization to which an object belongs.

LDAP Authentication Process

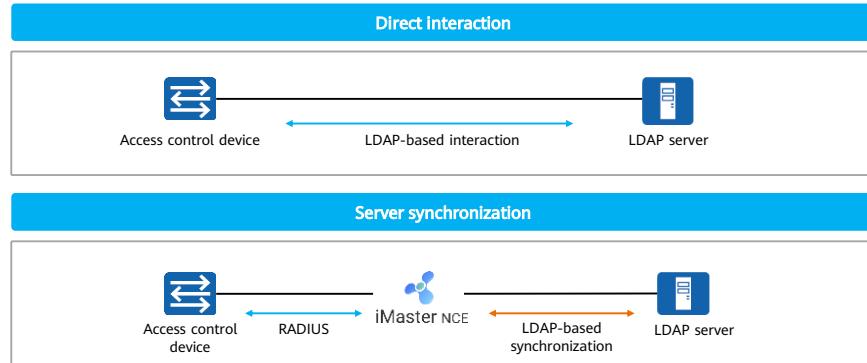


- The authentication process is as follows:

- The user enters the username and password to initiate a login request. The firewall establishes a TCP connection with the LDAP server.
- The firewall sends a bind request packet carrying the administrator's DN and password to the LDAP server in order to obtain the search permission.
- After the binding is successful, the LDAP server sends a bind response packet to the firewall.
- The firewall sends a user DN search request packet carrying the entered username to the LDAP server.
- The LDAP server searches for the user based on the user DN. If the search is successful, the LDAP server sends a search response packet.
- The firewall sends a user DN bind request packet carrying the obtained user DN and entered password to the LDAP server. The LDAP server then checks whether the password is correct.
- After the binding is successful, the LDAP server sends a bind response packet to the firewall.
- The LDAP server authorizes the user.
- After the authorization is successful, the firewall notifies the user that the login is successful.

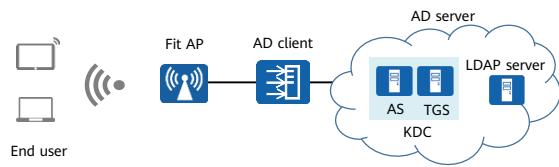
Typical LDAP Architecture

- Some network devices can directly interact with the LDAP server. In addition, iMaster NCE-Campus, as the authentication server, can act as a client to synchronize user information from the LDAP server. Therefore, for devices that cannot directly interact with the LDAP server, iMaster NCE-Campus can function as a client to synchronize user information from the LDAP server for user authentication.



Overview of AD

- Kerberos is a network authentication protocol that securely transmits data on an open network using a cipher key system. It does not require that all devices on a network be secure and assumes that all data may be read and modified during transmission. Kerberos runs over TCP and uses port 88.
- Kerberos provides a symmetrical key mechanism to improve password transmission security. Therefore, integrating the Kerberos protocol into LDAP authentication can prevent user password leakage during LDAP authentication. This authentication mode integrated with the Kerberos protocol is called AD authentication.
- Kerberos can be used for interconnection between network access devices and the AD server.



Components of the AD server

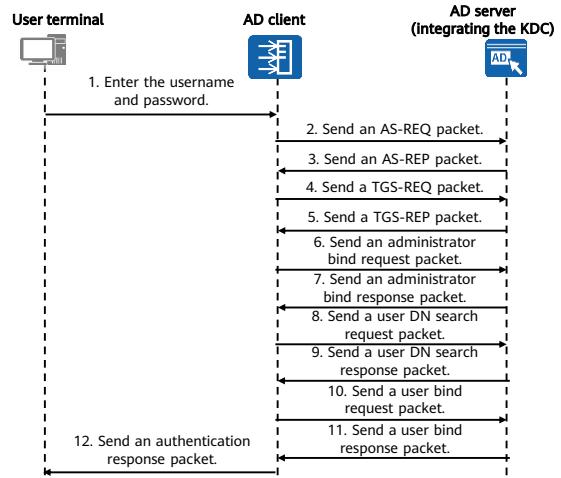
- LDAP server: stores all directory information.
- Key Distribution Center (KDC): Kerberos server, which stores all password and account information of clients. The KDC consists of AS and TGS.
- Authentication Server (AS): provides the tickets used to access TGS.
- Ticket-Granting Server (TGS): provides the tickets used to access the AD server.

- AD client: an access device integrating Kerberos and LDAP.
- AD server: a server integrating Kerberos and LDAP authentication. Generally, an AD server is the combination of an LDAP server and a Kerberos server.

AD Authentication and Authorization Process

- Compared with the authentication and authorization processes of LDAP, those of AD have added the following encryption and decryption processes:

 - An AS-REQ packet carrying the cleartext username is sent to the Kerberos server.
 - The AS server returns an AS-REP packet to the client. The ticket in the AS-REP packet is encrypted using the shared key of the AS and TGS servers, and the encrypted ticket and session key are encrypted again using the client password.
 - The AD client uses its own password to decrypt the AS-REP packet and obtains the session key and encrypted ticket.
 - The Kerberos server decrypts the ticket using the shared key of the AS and TGS servers, extracts the session key from the ticket, and decrypts the authenticator using the session key. If the client name and time in the authenticator are the same as those in the ticket, the authentication is successful and the Kerberos server sends an REP packet.

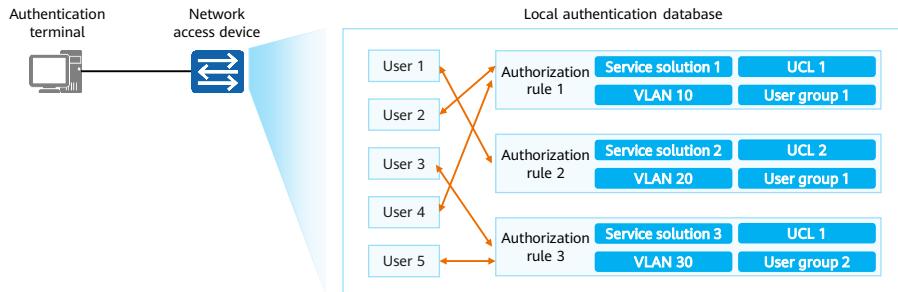


- If a user needs to access the AD server, the user initiates an authentication request and sends the username and password to the AD client.
- If the AD client accesses the AD server for the first time, the Kerberos server integrated in the AD server needs to authenticate the client. The client sends an AS-REQ packet carrying the cleartext username to the Kerberos server.
- The Kerberos server searches for the user in the database according to the obtained username. If the user is found, the AS server generates a session key shared between the Kerberos server and client. In addition, the AS server generates a ticket. The AD client uses this ticket to request for the ticket for accessing the AD server from the Kerberos server. In this case, the AD client does not need to be authenticated. The AS server returns an AS-REP packet to the client. The ticket in the AS-REP packet is encrypted using the shared key of the AS and TGS servers, and the encrypted ticket and session key are encrypted again using the client password.
- The AD client uses its own password to decrypt the AS-REP packet and obtains the session key and encrypted ticket. The AD client sends a TGS-REQ packet to the Kerberos server to request the ticket for accessing the AD server. The packet contains the authenticator, encrypted ticket, client name, and AD server name. An authenticator refers to the information, such as client username, IP address, time, and domain name, encrypted using the session key.

- The Kerberos server decrypts the ticket using the shared key of the AS and TGS servers, extracts the session key from the ticket, and decrypts the authenticator using the session key. If the client name and time in the authenticator are the same as those in the ticket, the authentication is successful. Then the Kerberos server returns a TGS-REP packet encrypted using the client password to the client. The packet contains the session key shared by the client and AD server and the ticket encrypted using the AD server password. The ticket contains information including the session key, client name, server name, and ticket validity period. The Kerberos client uses its own password to decrypt the TGS-REP packet and obtains the session key shared by the client and AD server and the ticket encrypted using the AD server password. The ticket can be used to access the AD server.
- Steps 6 to 12 in the authentication and authorization processes of AD are similar to steps 2 to 8 in those of LDAP. The difference is that in step 10 of AD authentication and authorization process, the session key and ticket are used to encrypt and verify the user password, which improves authentication security. The user bind request packet in step 10 contains the authenticator used by the AD client to encrypt the username and password (using the session key) and the ticket (encrypted using the AD server password) for accessing the AD server.
- After receiving the user bind request packet, the AD server uses its own password to decrypt the ticket, and checks whether the ticket is within the validity period. If the ticket does not expire, the AD server uses the session key carried in the ticket to decrypt the authenticator, processes the user bind request packet, and verifies whether the password entered by the user is correct.

Local Authentication and Authorization

- User identity authentication and authorization can be performed on the access control device or the server. If user identity authentication and authorization are performed on the access control device, a local user authentication server is configured on the access control device.
- Local authentication features fast processing and low operational costs. However, the information storage capacity is subject to the device hardware. Therefore, this mode is usually used for device login authentication.



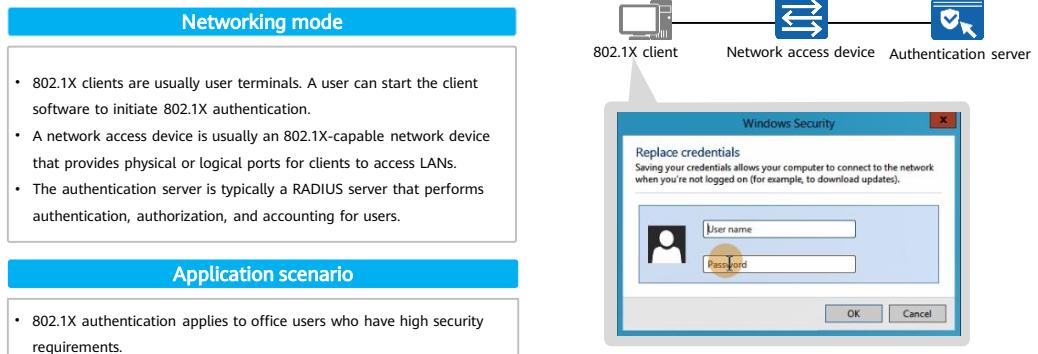
- Local authorization supports parameters including VLAN, service-scheme, and user group (or UCL).
- service-scheme: contains a series of network resources. When a service scheme is authorized to a user, the corresponding resources are granted to the user. The supported network resources are as follows:
 - ACL: specifies the range of network resources that can be accessed by a user.
 - User-VLAN: authorization VLAN of a user.
 - Admin-user privilege level: specifies the administrator level of a user who logs in to the device as an administrator.
 - Other parameters: DNS address, the maximum number of access users using the same username, etc.
 - UCL: a set of users with the same attributes, for example, users with partially same or the same network access permissions. The user control list (UCL) group can be used as a condition to restrict subsequent implementation of access control policies. If an ACL is used to restrict network access permissions, a UCL group can be used as a source or destination matching condition.

Contents

1. Overview of NAC
2. User Identity Authentication
- 3. Access Authentication**
 - 802.1X Authentication
 - Portal Authentication
 - MAC Address Authentication
 - Multi-Mode Authentication
 - User Authorization
4. NAC Configuration

802.1X Authentication

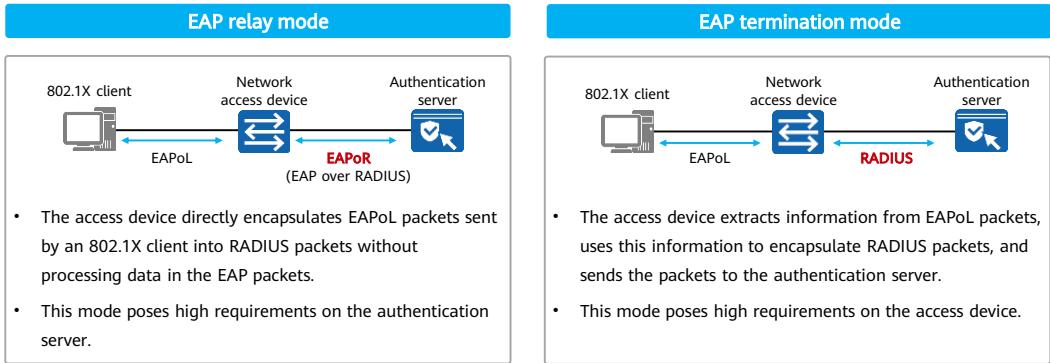
- 802.1X authentication is a port-based network access control technology. User identities are verified and network access permissions are controlled on ports of access devices. 802.1X authentication uses the Extensible Authentication Protocol (EAP) to exchange authentication information between the client, access device, and authentication server.



- 802.1X is a Layer 2 protocol and does not involve Layer 3 processing. It does not require access devices to provide high performance, reducing network construction costs.
- 802.1X authentication packets and data packets are transmitted through different logical ports, improving security.

802.1X Authentication Mode

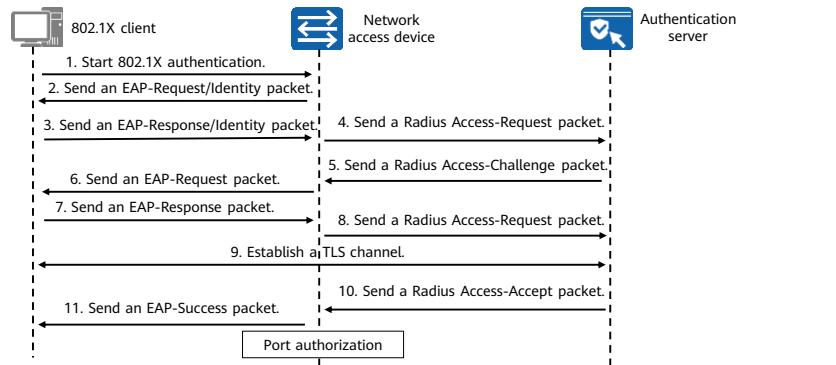
- Based on the mechanism used by the access device to process EAPoL packets sent by 802.1X clients, authentication modes can be classified into EAP relay mode and EAP termination mode.



- EAP relay mode
 - This mode simplifies processing on the access device and supports multiple authentication methods. However, the authentication server must support EAP and have high processing capability.
 - The most commonly used authentication modes include EAP-TLS, EAP-TTLS, and EAP-PEAP, of which EAP-TLS is the most secure because it requires a certificate to be loaded on both the client and authentication server. EAP-TTLS and EAP-PEAP are easier to deploy but less secure than EAP-TLS since the certificate needs to be loaded only on the authentication server and not the client.
- EAP termination mode
 - This mode is advantageous in that mainstream RADIUS servers support both PAP and CHAP authentication, eliminating the need for server upgrade. However, the workload on the access device is heavy because it needs to extract client authentication information from the EAP packets sent by the client and encapsulate the information using the standard RADIUS protocol. Furthermore, the access device does not support other EAP authentication methods except MD5-Challenge.
 - The major difference between PAP and CHAP is that in CHAP authentication, passwords are transmitted in ciphertext, whereas in PAP authentication, passwords are transmitted in cleartext. Therefore, PAP authentication has low security, and CHAP authentication is usually used in actual applications.

802.1X Authentication Process

- 802.1X authentication can be triggered in either of the following modes: The client sends an EAPoL-Start packet or the client associates with the network access device.
- The following figure shows the 802.1X authentication process in EAP relay mode where 802.1X authentication is triggered by association between the client and network access device.



29 Huawei Confidential

HUAWEI

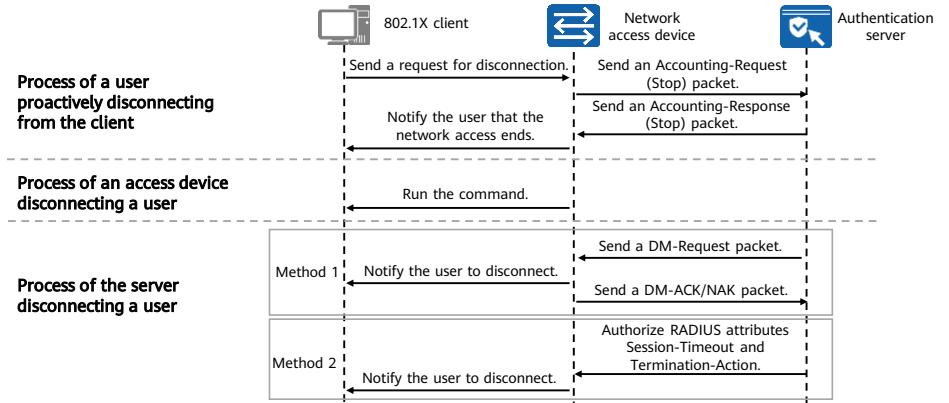
- Authentication process in EAP relay mode:

1. The client associates with the access device to trigger 802.1X authentication.
2. The access device sends an identity request packet (EAP-Request/Identity) to request the identity information of the client.
3. The client responds to the request sent by the access device and sends the identity information to the access device through an identity response packet (EAP-Response/Identity).
4. The access device encapsulates the EAP packet in the response packet sent by the client into a RADIUS packet (RADIUS Access-Request) and sends the packet to the authentication server for processing.
5. After receiving the user identity information from the access device, the RADIUS server starts to negotiate the EAP authentication method with the client. The RADIUS server encapsulates the EAP authentication method into a RADIUS Access-Challenge packet, and sends the packet to the access device.
6. The access device forwards the EAP information in the received RADIUS Access-Challenge packet to the client.

7. The client parses the received EAP information to obtain the EAP authentication method. If the client supports this method, it sends an EAP-Response packet encapsulated with this method to the access device. If the client does not support this method, it encapsulates an EAP-Response packet with the EAP authentication method it supports, and sends the packet to the access device.
8. The access device encapsulates a RADIUS packet with the EAP information carried in the received EAP-Response packet, and sends the RADIUS packet to the RADIUS server.
9. After the RADIUS server receives the packet, if the authentication method selected by the client is the same as that selected by the server, negotiation of the EAP authentication method succeeds and the authentication starts. Take EAP-PEAP authentication method as an example, the server encapsulates its certificate into a RADIUS packet and sends the packet to the access device. After receiving the packet, the access device forwards the certificate information to the client. The client verifies the server certificate (optional), negotiates TLS parameters with the RADIUS server, and establishes a TLS tunnel with the server. This tunnel is used to transmit TLS-encrypted user information among the client, access device, and RADIUS server. If negotiation of the EAP authentication method between the client and server fails, the authentication process is terminated, and the access device is notified of the authentication failure and disconnects the client.
10. After authenticating the client, the RADIUS server notifies the access device of successful authentication and delivers the key for handshake between the access device and client.
11. After receiving the RADIUS Access-Accept packet, the access device sends an EAP-Success packet to the client, changes the access port state of the user to authorized, and allows the user to access the network through this port. The access device performs handshake with the client using the key received from the RADIUS server. When the handshake is successful, the client successfully associates with the access device.
 - In EAP termination mode, the access device negotiates the EAP authentication method with the client, and sends user information to the RADIUS server for authentication. In contrast, such negotiation in EAP relay mode is performed between the client and server; the access device is only responsible for encapsulating EAP packets into RADIUS packets and transparently transmitting the RADIUS packets to the authentication server. The authentication server performs the entire authentication process.

Disconnecting 802.1X Authentication Users

- A user may be disconnected in the following modes: a user proactively disconnects from the client, the access device disconnects a user, and the server disconnects a user.



31 Huawei Confidential

HUAWEI

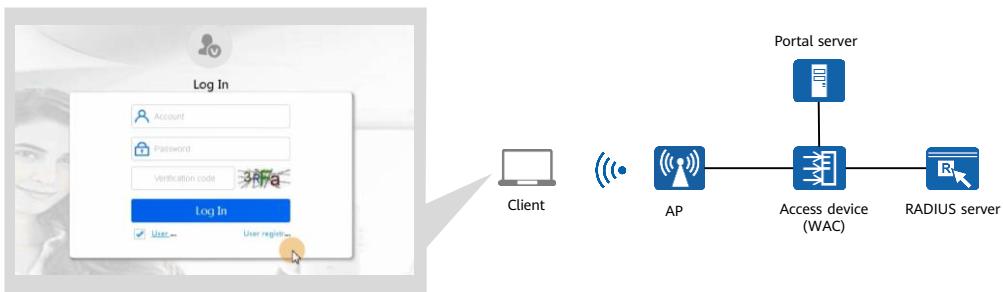
- The access device disconnects a user:
 - Run the corresponding command on the access device to disconnect a specified user. If the administrator detects that an unauthorized user is online or wants to disconnect a user and then bring the user online again during a test, the administrator can run the corresponding command on the access device to disconnect the user.
- The server can disconnect a user using the following methods:
 - The RADIUS server sends a Disconnect Message (DM) to disconnect a user. DM refers to the packet proactively sent by the RADIUS server to disconnect a user.
 - The RADIUS server authorizes the standard RADIUS attributes Session-Timeout and Termination-Action. Session-Timeout specifies the online duration timer of a user. If the value of Termination-Action is 0, the user is disconnected. When the online duration of a user reaches the value specified by the timer, the device disconnects the user.

Contents

1. Overview of NAC
2. User Identity Authentication
- 3. Access Authentication**
 - 802.1X Authentication
 - Portal Authentication
 - MAC Address Authentication
 - Multi-Mode Authentication
 - User Authorization
4. NAC Configuration

Portal Authentication

- Portal authentication is also called web authentication. Users can enter their usernames and passwords on the web authentication page for identity authentication. Users can access the authentication page in either of the following ways:
 - Proactive authentication: A user proactively accesses the Portal authentication website through browsers.
 - Redirected authentication: If the access address entered by a user is not the address of the Portal authentication website, the access device forcibly redirects the user to the Portal authentication website.



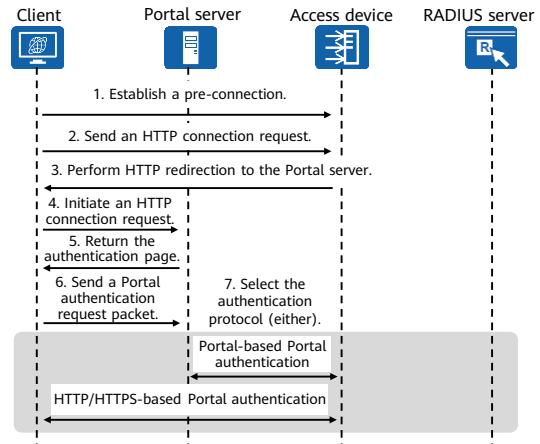
33 Huawei Confidential

 HUAWEI

- Client: In most cases, a client is a host where an HTTP/HTTPS-capable browser is installed. Sometimes, corresponding client software (such as browsers) is installed.
- Access device: a network device such as a switch or router, which provides the following functions:
 - Redirects all HTTP and HTTPS requests of users on authentication network segments to the Portal server before authentication is performed.
 - Interacts with the Portal server and authentication server to implement user identity authentication, authorization, and accounting during authentication.
 - Grants users access to the network resources authorized by the administrator upon successful authentication.
- Portal server: a server system that receives authentication requests from clients, provides Portal services and authentication pages, and exchanges client authentication information with access devices.
- Authentication server: interacts with access devices to implement user authentication, authorization, and accounting.
- Portal authentication does not require dedicated client software. Therefore, it is typically used in access scenarios requiring no client software or guest access scenarios.

Portal Authentication Protocol

- The Portal protocol includes:
 - Portal access protocol: HTTP/HTTPS, which describes the protocol interaction between clients and the Portal server.
 - Portal authentication protocols:
 - Portal protocol: describes the protocol interaction between the Portal server and access devices. It is used to transfer parameters such as the username and password. It is compatible with the Portal 2.0 protocol of China Mobile, and supports the basic functions of the protocol.
 - HTTP or HTTPS protocol: describes the protocol interaction between clients and access devices. It is used to transfer parameters such as the username and password.



34 Huawei Confidential

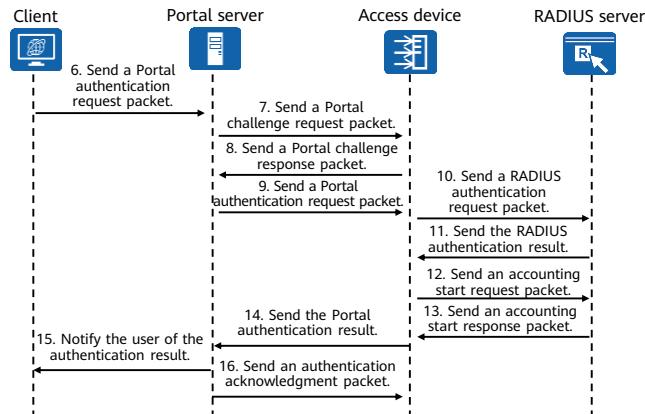
HUAWEI

- The Portal authentication process is as follows:

1. Before the authentication, the client establishes a pre-connection with the access device. That is, the access device has established a user online entry for the client before the authentication succeeds and the client is granted access to some network resources.
2. The client initiates an HTTP connection request.
3. The access device receives the HTTP connection request packet and determines whether to permit the packet. It permits an HTTP packet destined for either the Portal server or configured non-authentication network resources and redirects the Uniform Resource Locator (URL) address of an HTTP packet destined for other addresses to the Portal authentication page.
4. The client initiates an HTTP connection request to the Portal server based on the obtained URL.
5. The Portal server returns the Portal authentication page to the client.
6. After the user enters the username and password on the Portal authentication page, the client sends a Portal authentication request to the Portal server.
7. Parameters such as the username and password are transferred according to the protocol interaction process specified by different authentication protocols.

Portal Authentication Process (1/2) — Portal

- Here, CHAP authentication is used as an example to describe the process of Portal-based Portal authentication.



35 Huawei Confidential

HUAWEI

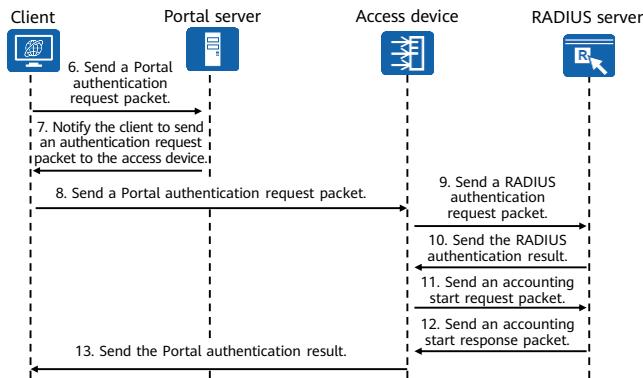
- The detailed authentication process is as follows:

- The Portal server receives the Portal authentication request. If CHAP authentication is used between the Portal server and access device, the Portal server sends a Portal challenge request packet (REQ_CHALLENGE) to the access device. If PAP authentication is used between the Portal server and access device, the access device goes to step 9.
- The access device sends a Portal challenge response packet (ACK_CHALLENGE) to the Portal server.
- The Portal server encapsulates the entered username and password into a Portal authentication request packet (REQ_AUTH) and sends the packet to the access device.
- The access device sends a RADIUS authentication request packet (ACCESS-REQUEST) to the RADIUS server based on the obtained username and password.
- The RADIUS server authenticates the username and password. If authentication succeeds, the RADIUS server sends an authentication accept packet (ACCESS-ACCEPT) to the access device. If authentication fails, the RADIUS server sends an authentication reject packet (ACCESS-REJECT) to the access device. The authentication accept packet contains authorization information because RADIUS provides both authentication and authorization functions.
- The access device permits or denies the user access based on the received authentication result. If user access is permitted, the access device sends an accounting start request packet (ACCOUNTING-REQUEST) to the RADIUS server.

13. The RADIUS server replies with an accounting start response packet (ACCOUNTING-RESPONSE), starts accounting, and adds the user to the local online user list.
14. The access device returns the Portal authentication result (ACK_AUTH) to the Portal server and adds the user to the local online user list.
15. The Portal server sends the authentication result to the client to notify the user of an authentication success and adds the user to the local online user list.
16. The Portal server sends an authentication acknowledgment packet (AFF_ACK_AUTH) to the access device.

Portal Authentication Process (2/2) — HTTP/HTTPS

- The following figure shows the packet exchange process of HTTP authentication during a user's going online. The packet exchange process of HTTPS authentication is similar but differs in that HTTPS packets are encrypted and decrypted.



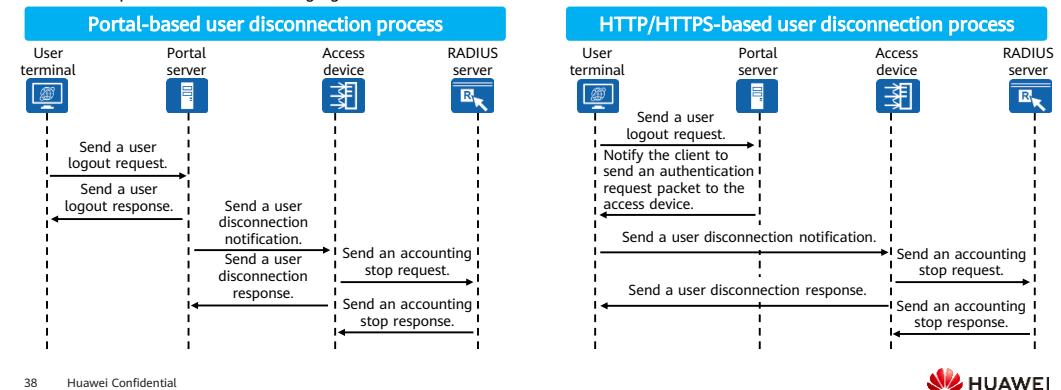
37 Huawei Confidential

HUAWEI

- The detailed authentication process is as follows:
 7. The Portal server notifies the client to send a Portal authentication request packet to the access device.
 8. The client sends a Portal authentication request packet (HTTP POST/GET) to the access device.
 9. The access device sends a RADIUS authentication request packet (ACCESS-REQUEST) to the RADIUS server based on the obtained username and password.
 10. The RADIUS server authenticates the username and password. If authentication succeeds, the RADIUS server sends an authentication accept packet (ACCESS-ACCEPT) to the access device. If authentication fails, the RADIUS server sends an authentication reject packet (ACCESS-REJECT) to the access device. The authentication accept packet contains authorization information because RADIUS provides both authentication and authorization functions.
 11. The access device permits or denies the user access based on the received authentication result. If user access is permitted, the access device sends an accounting start request packet (ACCOUNTING-REQUEST) to the RADIUS server.
 12. The RADIUS server replies with an accounting start response packet (ACCOUNTING-RESPONSE), starts accounting, and adds the user to the local online user list.
 13. The access device returns the Portal authentication result to the client and adds the user to the local online user list.

Disconnecting Portal Authentication Users (1/2) — A User Proactively Disconnecting from the Client

- A user initiates a disconnection request. For example, if the user clicks the logout button, the client sends a logout request to the Portal server.
- The process of Portal-based proactive disconnection differs from that of the HTTP/HTTPS-based proactive disconnection, and the details are provided in the following figure.



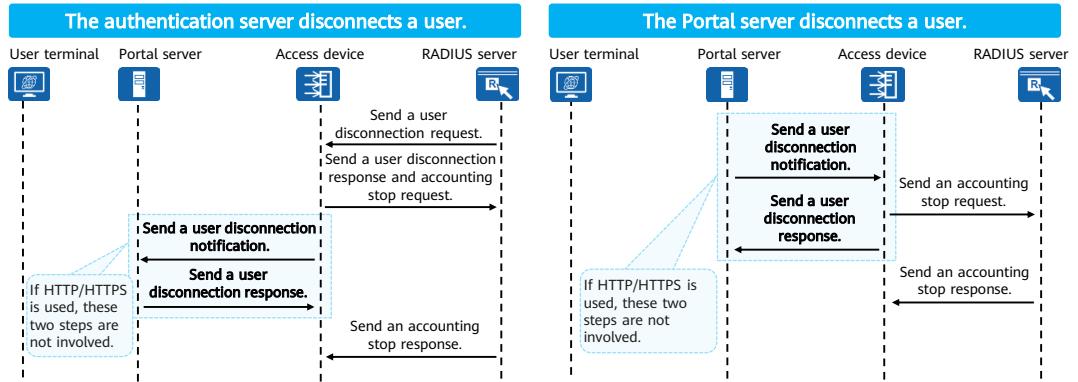
38 Huawei Confidential

HUAWEI

- A user may be disconnected in the following modes:
 - A user proactively disconnects from the client.
 - The access device disconnects a user.
 - The server disconnects a user.

Disconnecting Portal Authentication Users (2/2) — The Server Disconnecting a User

- In Portal authentication networking, two types of servers are involved: authentication server and Portal server. Both of them can disconnect users and the processes are as follows:



39 Huawei Confidential

 HUAWEI

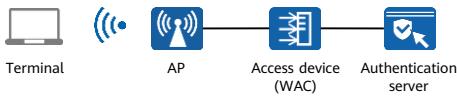
- Portal authentication also allows the access device to disconnect users. That is, the access device directly delivers a command to disconnect users.

Contents

1. Overview of NAC
2. User Identity Authentication
- 3. Access Authentication**
 - 802.1X Authentication
 - Portal Authentication
 - MAC Address Authentication**
 - Multi-Mode Authentication
 - User Authorization
4. NAC Configuration

MAC Address Authentication

- MAC address authentication (MAC authentication for short) controls network access permissions of users based on ports and MAC addresses. User terminals are authenticated by the authentication server based on their MAC addresses.
- By default, a switch triggers MAC authentication for users after receiving a DHCP, ARP, DHCPv6, or ND packet. You can also configure the switch to trigger MAC authentication after receiving any data frame.

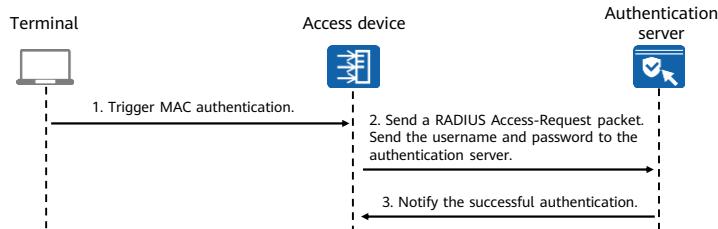


- Terminal: refers to a terminal that attempts to access the network.
- Access device: functions as the network access control point that enforces security policies. It permits, denies, isolates, or restricts network access of users based on the security policies customized for customer networks.
- Authentication server: checks whether the identities of users who attempt to access the network are valid and assigns network access permissions to users who have valid identities.

- MAC authentication does not require users to install any client software. It applies to scenarios where dumb terminals such as IP phones and printers need to access the network.
- Dumb terminal: Compared with other terminals, dumb terminals have limited functions and simple interaction modes. Its specific meaning varies according to the scenario (context). Here, dumb terminals refer to terminals that do not support entering authentication information such as usernames and passwords.
- Advantages of MAC authentication:
 - No client software needs to be installed on user terminals.
 - During MAC authentication, users do not need to enter usernames or passwords.
 - Dumb terminals that do not support 802.1X authentication, such as printers and fax machines, can be authenticated.

MAC Authentication Process

- Passwords of MAC authentication users can be processed using PAP or CHAP.
 - PAP: The access device arranges the MAC address, shared key, and random value in sequence, performs hash processing on them using the MD5 algorithm, and encapsulates the hash result into the User-Password attribute.
 - CHAP: The access device arranges the CHAP ID, MAC address, and random value in sequence, performs hash processing on them using the MD5 algorithm, and encapsulates the hash result into the CHAP-Password and CHAP-Challenge attributes.



42 Huawei Confidential

HUAWEI

- MAC authentication process in PAP mode:

1. The access device receives a DHCP, ARP, DHCPv6, or ND packet from a terminal, which triggers MAC authentication.
 2. The access device generates a random value, arranges the terminal MAC address, shared key, and random value in sequence, and performs hash processing on them using the MD5 algorithm. It then encapsulates the user name, hash result, and random value into a RADIUS Access-Request packet, and sends the packet to the RADIUS server for MAC authentication.
 3. Based on the received random value, the RADIUS server performs hash processing on the combination of the user MAC address, shared key, and random value in the local database using the MD5 algorithm. If the hash result is the same as that carried in the received packet, the RADIUS server sends an Access-Accept packet to the access device, indicating that MAC authentication of the user is successful. The user is then allowed to access the network.
- MAC authentication in CHAP and PAP modes differs in that in the CHAP mode, the CHAP ID, MAC address, and random value of a MAC authentication user are arranged in sequence and then encrypted using the MD5 algorithm.
 - The modes of disconnecting a MAC authentication user are similar to those of disconnecting an 802.1X authentication user:
 - A user proactively disconnects from the client.
 - The access device disconnects a user.
 - The server disconnects a user.
 - Details are not described here.

Comparison Between Three Authentication Modes

- The three authentication modes have different authentication principles and are applicable to different scenarios. In actual applications, you can use a proper authentication mode or multiple authentication modes based on scenarios.

Item	802.1X Authentication	MAC Authentication	Portal Authentication
Application scenario	New networks with concentrated users and high security requirements	Authentication of dumb terminals such as printers and fax machines	Scenarios with scattered and moving users
Client requirement	Required	Not required	Not required
Advantage	High security	No client required	Flexible deployment
Disadvantage	A dedicated authentication server needs to be deployed, which is complex.	MAC addresses need to be registered, complicating management.	Low security

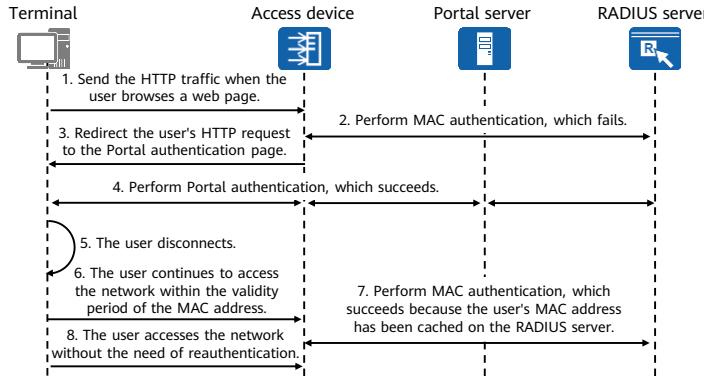
- Currently, the following multi-mode authentication modes are supported:
 - MAC address-prioritized Portal authentication
 - MAC + 802.1X multi-mode authentication

Contents

1. Overview of NAC
2. User Identity Authentication
- 3. Access Authentication**
 - 802.1X Authentication
 - Portal Authentication
 - MAC Address Authentication
 - Multi-Mode Authentication**
 - User Authorization
4. NAC Configuration

Multi-Mode Authentication (1/2) — MAC Address-Prioritized Portal Authentication

- MAC address-prioritized Portal authentication allows disconnected users who have passed Portal authentication to access the network again within a certain period of time, without having to reenter their usernames and passwords, as long as they pass MAC authentication.



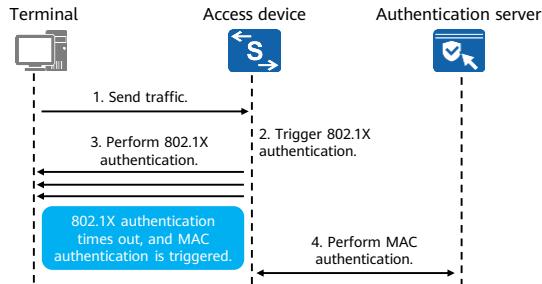
45 Huawei Confidential

HUAWEI

- MAC address-prioritized Portal authentication solves the problem that after passing Portal authentication in a wireless environment, end users are disconnected due to unstable wireless signals or leaving the current wireless signal coverage area. In this case, end users need to frequently enter their usernames and passwords in the web browser for reauthentication to access the network.
- To use this function, you need to configure MAC + Portal multi-mode authentication on the device, and enable MAC address-prioritized Portal authentication and configure the MAC address validity period on the authentication server.

Multi-Mode Authentication (2/2) — MAC Address Bypass Authentication

- When PCs and dumb terminals such as printers and fax machines are connected to an interface of an access device, you can configure MAC address bypass authentication so that dumb terminals that do not support 802.1X authentication can access the network through MAC authentication.
- MAC address bypass authentication takes longer than MAC authentication because it has an additional 802.1X authentication stage.



46 Huawei Confidential

HUAWEI

- MAC address bypass authentication applies only to terminals that access the network in wired mode. Either successful MAC authentication or 802.1X authentication means that the user is authenticated. When a terminal accesses the network in wireless mode, multi-mode authentication (MAC + 802.1X authentication) is used. MAC authentication is first performed on the terminal. After the MAC authentication succeeds, 802.1X authentication is performed. The user is authenticated after both of the authentication are passed. For details, see the authentication process of 802.1X authentication and MAC authentication.

Contents

1. Overview of NAC
2. User Identity Authentication
- 3. Access Authentication**
 - 802.1X Authentication
 - Portal Authentication
 - MAC Address Authentication
 - Multi-Mode Authentication
 - User Authorization**
4. NAC Configuration

User Authorization

- Using RADIUS server authorization as an example, the typical authorization information includes:
 - VLAN: To prevent unauthenticated users from accessing restricted network resources, the restricted network resources and unauthenticated users are usually divided into different VLANs. After a user is authenticated, the authentication server authorizes a specified VLAN to the user.
 - ACL: After a user is authenticated, the authentication server authorizes a specified ACL to the user. Then the access device controls the user's packets according to the ACL.
 - UCL: A user control list group is a collection of network members. Members in a UCL group can be network terminals such as PCs and mobile phones. The administrator can add users requiring the same network access policy to the same UCL group, and configure a network access policy for the UCL group. Compared with the solution in which network access control policies are deployed for each user, the UCL group-based network access control solution greatly reduces the workload of administrators.

Status	802.1X	MAC Authentication	Portal Authentication
Dynamic VLAN	✓	✓	✗
Dynamic ACL	✓	✓	✓
UCL	✓	✓	✓

- Because RADIUS provides both authentication and authorization functions, when a RADIUS server is used for authentication, the authentication accept packet contains authorization information.
- Authorization VLAN: After a user is authenticated, the authentication server authorizes a specified VLAN to the user. At this time, the access device changes the VLAN to which the user belongs to the authorized VLAN, without changing the interface configuration. However, the authorized VLAN takes precedence over the VLAN configured by the user. That is, the authorized VLAN takes effect after the user is authenticated, and the VLAN configured by the user takes effect after the user is disconnected.
- The RADIUS server can authorize an ACL to a user using either of the following methods:
 - Static ACL authorization: The RADIUS server uses the standard RADIUS attribute Filter-Id to authorize an ACL ID to a user. To make the authorized ACL take effect, you need to configure the corresponding ACL and ACL rules on the access device in advance.
 - Dynamic ACL authorization: The RADIUS server uses the Huawei extended RADIUS attribute HW-Data-Filter to authorize an ACL ID and ACL rules to a user. The ACL ID and ACL rules need to be configured only on the RADIUS server instead of the access device.

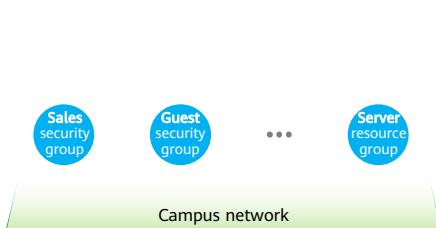
- The RADIUS server can authorize a UCL group to a user using either of the following methods:
 - UCL group name authorization: The RADIUS server uses the standard RADIUS attribute Filter-Id to authorize a UCL group name to a specified user.
 - UCL group ID authorization: The RADIUS server uses the Huawei extended RADIUS attribute HW-UCL-Group to authorize a UCL group ID to a specified user.
 - You must configure the UCL group and its network access policy on the device in advance regardless of which UCL group authorization method is used.

Authentication-free and Authentication Event Authorization

Authentication-free (free-rule)	Authentication event authorization
<p>Before user authentication, authentication-free rules can be defined to grant users some basic network access permissions, such as downloading the 802.1X client and updating the antivirus database.</p> <p>Authentication-free rule profile</p> <p>Method 1: common authentication-free rule, which is determined by parameters such as IP address, MAC address, source interface, and VLAN</p> <p>Method 2: ACL association</p> <p>The user can access 192.168.1.1 without authentication.</p> <p>User terminal → Access device → Software server 192.168.1.1</p> <p>Allow users to access 192.168.1.1 to download the client before successful authentication.</p>	<p>When encountering different events during authentication (for example, a user fails to be authenticated or the authentication server fails), users still need to have certain access permissions.</p> <p>Authorization parameters</p> <p>VLAN: Users are granted access permissions to resources in the corresponding VLAN.</p> <p>UCL: Permissions are delivered to users with the same characteristics based on the UCL group.</p> <p>service-scheme: Parameters such as UCL, VLAN, and QoS-profile can be bound to a service scheme.</p> <p>User terminal → Access device → Antivirus server 192.168.1.1</p> <p>The user can still access 192.168.1.1 after the authentication fails.</p> <p>Allow users to access 192.168.1.1 to update the antivirus database after authentication failures.</p>

- The authorization mode based on the authentication event (generally, authorization in the scenario where authentication fails) is also called the bypass mode. Different authentication modes have different bypass schemes. Some bypass schemes are shared, while some are supported only by specific authentication modes. For details, see contents related to NAC bypass in the corresponding product documentation.

Security Group



What is a security group?

1. A security group is a collection of users or resources that have the same network access policy. Security groups are related only to user identities, and are completely decoupled from network information such as user VLANs and IP addresses.
2. Security groups can be authorized to users based on 5W1H conditions. Users meeting 5W1H conditions can be authorized to specified security groups (dynamic security groups). You can also define security groups (static security groups) through statically binding IP addresses.

What is a resource group?

1. Administrators can specify static IP addresses of servers in security groups to add the servers to security groups. However, service resources with overlapping IP addresses cannot be differentiated using security groups.
2. Resource groups are introduced to address the problem. IP addresses specified in resource groups can overlap, and resource groups can be configured as destination groups of inter-group access control policies.

- 5W1H:
 - Who: indicates the identity of an access user, for example, a corporate executive, an employee, or a guest.
 - Where: indicates the access location of a user, for example, inside a campus.
 - What: indicates the type of the terminal used by an access user, for example, a mobile phone, PC, or laptop.
 - When: indicates the time when a user accesses the network, for example, in the daytime or at night.
 - Whose: indicates the device ownership, for example, a company terminal or a personal terminal.
 - How: indicates the user access mode, for example, wired or wireless access.

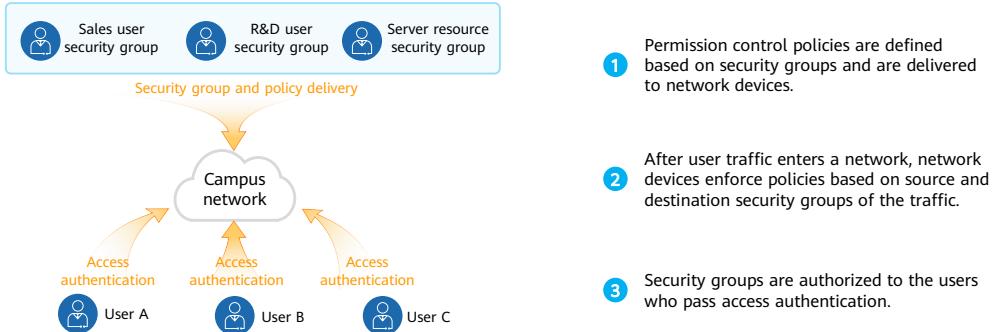
Policy Control

- After security groups and resource groups are defined, administrators can define inter-group network-wide access control policies based on the security groups and resource groups.
- The inter-group control policies are presented in a policy matrix. The inter-group control policies mainly control access between groups.

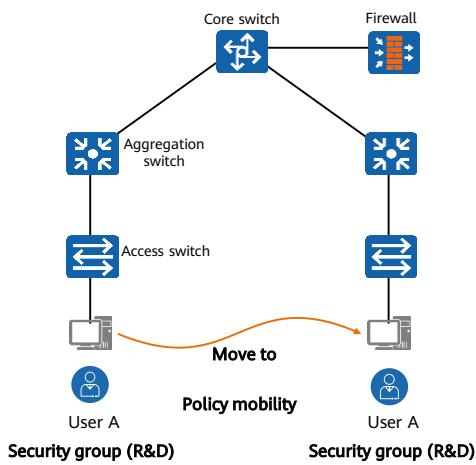
Source Security Group	Destination Group	g_employee	g_guest	unknown	any
g_employee			✓		
g_guest		✗			
unknown					

Security Group-based Policy Management

- Security group-based policy management: grants a user consistent network permissions and enforces the corresponding policies on the user regardless of the user's location and IP address.



Security Group-based Permission Control



User permission control

- User permission control is performed based on security groups.
- User communication permission control:
 - Communication permission control over users on the same authentication point
 - Communication permission control over users on different authentication points
- Resource access permission control
 - Permission control over access to internal and external network resources

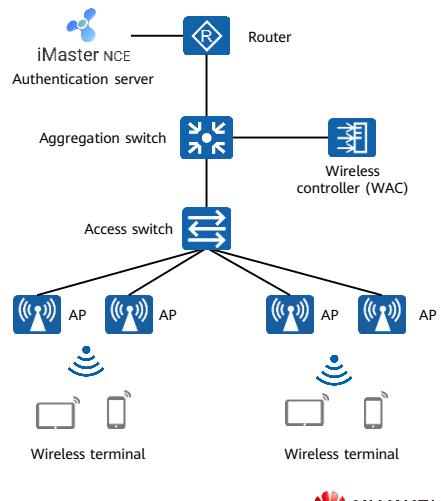
Contents

1. Overview of NAC
2. User Identity Authentication
3. Access Authentication
- 4. NAC Configuration**

Access Control Solution for Wireless Users

- Solution architecture
 - Client: terminals with wireless network adapters, such as laptops, mobile phones, and printers, which can wirelessly access the network.
 - Access device: wireless controller (WAC).
 - Network access control point for terminals.
 - Implements access control (permit, deny, isolate, or restrict) based on the security policies formulated by customer networks.
 - Enforcement point of authorization policies.
 - Authentication server: iMaster NCE-Campus
 - Checks whether the identity of the terminal that attempts to access the network is valid.
 - Specifies the network access permissions that a valid terminal can have.

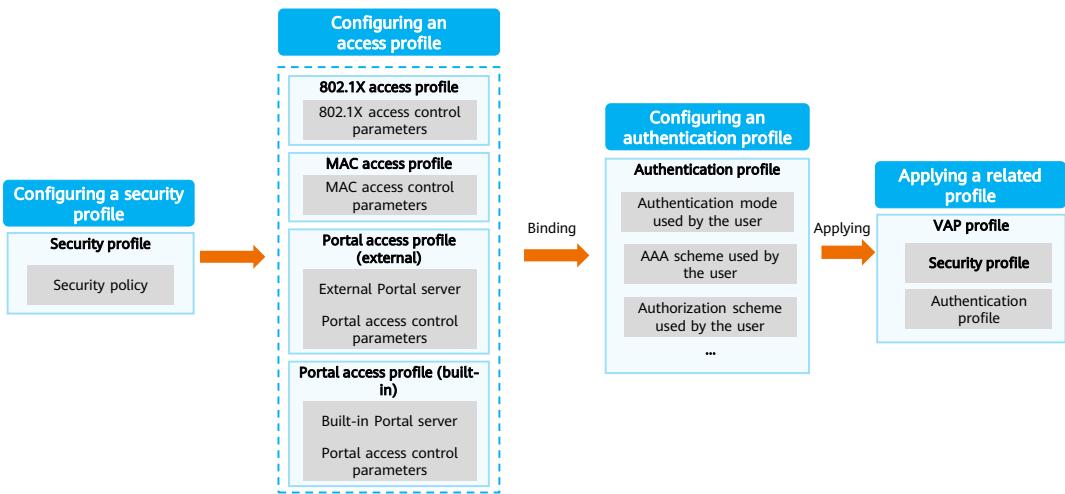
56 Huawei Confidential



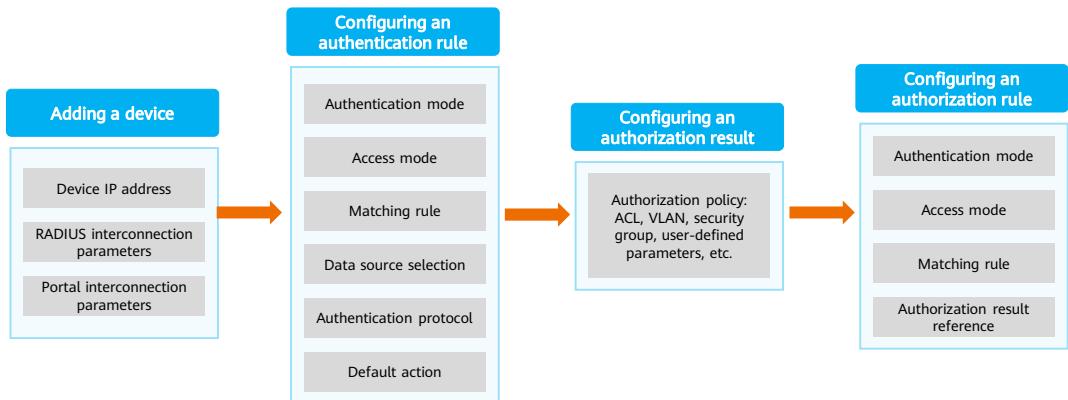
HUAWEI

- With the popularization of wireless devices, we have entered the fully-wireless office era which is wireless-centric. In the office environment, wired networks are replaced by wireless networks. Terminals such as laptops, mobile phones, and printers now mainly access the network in wireless mode. Therefore, this course describes the NAC configuration solution in wireless scenarios.

NAC Configuration Process (1/2) — WAC



NAC Configuration Process (2/2) — iMaster NCE-Campus



802.1X Authentication Configuration — WAC (1/2)

- Configure a security profile.

```
[WAC] wlan  
[WAC-wlan] security-profile name test  
[WAC-wlan-sec-prof-test] security wpa-wpa2 dot1x aes (security policy: WPA or WPA2-8021.X)  
[WAC-wlan-sec-prof-test] quit
```

- Configure an access profile.

```
[WAC] dot1x-access-profile name test  
[WAC-dot1x-access-profile-acc_test] quit
```

- Configure a RADIUS server.

```
[WAC] radius-server template test  
[WAC-radius-test] radius-server authentication X.X.X.X (IP address of the RADIUS server) 1812  
[WAC-radius-test] radius-server accounting X.X.X.X (IP address of the RADIUS server) 1813  
[WAC-radius-test] radius-server shared-key cipher Huawei@123 (shared key, which must be the same as that configured on the RADIUS server)  
[WAC-radius-test] quit  
[WAC] radius-server authorization X.X.X.X (IP address of the RADIUS server) shared-key cipher Huawei@123 (shared key)
```

802.1X Authentication Configuration — WAC (2/2)

- Configure an AAA scheme.

```
[WAC-aaa] authentication-scheme test  
[WAC-aaa-authen-test] authentication-mode radius  
[WAC-aaa] accounting-scheme test  
[WAC-aaa-authen-test] accounting-mode radius  
[WAC-aaa] domain test  
[WAC-aaa-domain-test] authentication-scheme test  
[WAC-aaa-domain-test] accounting-scheme test  
[WAC-aaa-domain-test] radius-server test
```

- Configure an authentication profile.

```
[WAC] authentication-profile name test  
[WAC-authentication-profile-test] dot1x-access-profile test  
[WAC-authentication-profile-test] access-domain test
```

- Apply the authentication profile and security profile.

```
[WAC-wlan-view] vap-profile name  
[WAC-wlan-vap-prof-dot1x] authentication-profile test  
[WAC-wlan-vap-prof-dot1x] security-profile test  
[WAC-wlan-vap-prof-dot1x] quit
```

802.1X Authentication Configuration — iMaster NCE-Campus (1/2)

- Add an admission device. Choose **Admission > Admission Resources > Admission Device > Admission Device Management**, click **Create** to add a WAC, as shown in the following figure.

The screenshot shows the 'Admission Device Management' section of the iMaster NCE-Campus interface. It includes tabs for 'Admission Regions' and 'Admission Device Template'. Under 'Third-party Admission Device', there is a table with columns for 'Device Name', 'Description', 'IP Address', 'Backup IP Address', 'Device Series', 'RADIUS Authent...', 'Portal Authent...', 'HWTACACS Aut...', and 'Operation'. A row for 'WAC1' is selected, showing its IP address as '10.23.100.1', status as 'Configured', and operation as 'Configured'. Buttons for 'Transfer', 'Export', 'Import', 'Delete', and 'Create' are visible at the top right.

- Add an authentication user. Choose **Admission > Admission Resources > User Management > User Management > User**, click **Create** to add a user, as shown in the following figure.

The screenshot shows the 'User Management' section of the iMaster NCE-Campus interface. It includes tabs for 'User Management', 'Role Management', and 'Blacklist Management'. Under 'User Management', there is a table with columns for 'Username', 'User Group', 'Role', 'Description', 'Email', 'Contact Number', 'Expiration Time', 'Enabled or Not', and 'Operation'. A row for 'dot1x-user' is selected, showing its role as 'ROOTHCIP...' and status as 'Enabled'. Buttons for 'Custom Field', 'Enable', 'Disable', 'Transfer', 'Delete', and 'Create' are visible at the top right.

- If the local data source is used as the data source in the authentication rule, you need to create an authentication user (by configuring information such as the username and password) on iMaster NCE-Campus. You can also use an external data source for account synchronization with the AD/LDAP server.

802.1X Authentication Configuration — iMaster NCE-Campus (2/2)

- Configure authentication and authorization rules, which can be matched by end users based on specific conditions.
 - Choose **Admission > Admission Policy > Authentication and Authorization > Authentication Rules**, modify the default authentication rule or create an authentication rule.

Admission / Admission Policy / Authentication and Authorization

Authentication Rules Authorization Result Authorization Rules Policy Element

Enter a name		Priority		Name		Authenticatio...		Access Mode		Matching Condition		Data Sour...		Authenticatio...		Access P...		Enabling Sta...		Operation		
<input type="checkbox"/>	1	<input type="checkbox"/>	802.1X	User access...	Wireless	<input type="checkbox"/>	User group	ROOTHCIP-WLAN	<input type="checkbox"/>	SSID	wlan-net	<input type="checkbox"/>	<Data sour...	EAP-PEAP...	<input type="checkbox"/>	Enable	<input type="checkbox"/>					

- Choose **Admission > Admission Policy > Authentication and Authorization > Authorization Rules**, associate the authorization result and specify the resources that can be accessed by authenticated users.

Admission / Admission Policy / Authentication and Authorization

Authentication Rules Authorization Result **Authorization Rules** Policy Element

Enter a name		Priority		Name		Authenticatio...		Access Mode		Matching Condition		Authorization...		Description		Enabling Sta...		Operation	
<input type="checkbox"/>	1	<input type="checkbox"/>	802.1X	User access...	Wireless	<input type="checkbox"/>	User group	ROOTHCIP-WLAN	<input type="checkbox"/>	SSID	wlan-net	<input type="checkbox"/>	Permit Access	<input type="checkbox"/>	Enable	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- The default authorization result of iMaster NCE-Campus can be used. To deliver a customized authorization result, you need to configure authorization result rules in advance.

Troubleshooting 802.1X Authentication Failures

- Check whether the **dot1x-access-profile** is bound to the authentication profile.
 - Error-prone configuration: **security wpa-wpa2 dot1x aes** is configured in the security profile. However, **dot1x-access-profile** is not bound to the authentication profile.
 - Suggestion: Bind the corresponding access profile to the authentication profile.
- Check whether the service VLAN is created on the WAC.
 - Error-prone configuration: In 802.1X authentication scenarios, EAP packets are control packets and need to be sent to the WAC through a CAPWAP tunnel. Therefore, the corresponding VLAN must be created on the WAC regardless of whether direct forwarding or tunnel forwarding is used.
 - Suggestion: Create the corresponding service VLAN on the WAC.
- To perform 802.1X authentication on different terminals, you need to perform certain operations. For details, see related documents on the Huawei official website.

Portal Authentication Configuration — WAC (1/2)

- Configure a security profile.

```
[WAC-wlan] security-profile name test  
[WAC-wlan-sec-prof-test] security open  
[WAC-wlan-sec-prof-test] quit
```

- Configure an access profile.

```
[WAC] url-template name portal  
[WAC-url-template-portal] url https://XXXX:19008/portal (IP address of the Portal server)  
[WAC-url-template-portal] url-parameter redirect-url redirect-url ssid ssid user-ipaddress userip user-mac umac device-ip ac-ip  
[WAC-url-template-portal] quit  
  
[WAC] web-auth-server portal  
[WAC-web-auth-server-portal] server-ip XXXX (IP address of the Portal server)  
[WAC-web-auth-server-portal] source-ip Y.YYY (IP address of the WAC)  
[WAC-web-auth-server-portal] share-key cipher Huawei@123 (shared key, which must be the same as that configured on the Portal server)  
[WAC-web-auth-server-portal] url-template portal  
[WAC-web-auth-server-portal] quit  
  
[WAC] portal-access-profile name portal  
[WAC-portal-access-profile-portal] web-auth-server portal direct  
[WAC-portal-access-profile-portal] quit
```

- The URL parameter names configured on the device must be the same as those supported by the Portal authentication server. iMaster NCE-Campus supports the following URL parameter names:
 - redirect-url**: The name can be url or redirect-url.
 - user-ipaddress**: The name can be userip.
 - user-mac**: The name can be usermac or umac.
 - ssid**: The name can be ssid.
 - device-ip**: The name can be ac-ip.
 - ap-mac**: The name can be apmac or ap-mac.

Portal Authentication Configuration — WAC (2/2)

- Configure the RADIUS server (same as the 802.1X authentication configuration).
- Configure an AAA scheme (same as the 802.1X authentication configuration).
- Configure an authentication profile.

```
[WAC] authentication-profile name portal  
[WAC-authentication-profile-portal] portal-access-profile portal  
[WAC-authentication-profile-portal] access-domain test  
[WAC-authentication-profile-portal] quit
```

- Apply the authentication profile and security profile.

```
[WAC-wlan-view] vap-profile name portal  
[WAC-wlan-vap-prof-portal] authentication-profile portal  
[WAC-wlan-vap-prof-portal] security-profile test  
[WAC-wlan-vap-prof-portal] quit
```

Portal Authentication Configuration — iMaster NCE-Campus

- Add an admission device. Choose **Admission > Admission Resources > Admission Device > Admission Device Management**, click **Create** to add a WAC. Both RADIUS authentication parameters and Portal authentication parameters need to be configured.
- The authentication, authorization, and user adding configurations are the same as those in 802.1X authentication.

<p>RADIUS authentication parameter:</p> <p>CoA Type: <input checked="" type="checkbox"/> Default CoA <input type="checkbox"/> No CoA <input type="checkbox"/> Port Bounce <input type="checkbox"/> Reauth</p> <p>CoA port: 3799</p> <p>Admission device template: <input type="text"/></p> <p>*Accounting key: <input type="text"/> <small>.....</small></p> <p>*Confirm accounting key: <input type="text"/> <small>.....</small></p> <p>*Authorization key: <input type="text"/> <small>.....</small></p> <p>*Confirm authorization key: <input type="text"/> <small>.....</small></p> <p>*Accounting interval (min): 3</p> <p>Custom MAC authentication password: <input checked="" type="checkbox"/></p> <p>Service-Type settings: <input checked="" type="checkbox"/></p>	<p>Portal authentication parameter:</p> <p>Portal protocol: <input checked="" type="checkbox"/> Huawei Portal(Portal2.0) <input type="checkbox"/></p> <p>Online portal user synchronization: <input checked="" type="checkbox"/> <input type="checkbox"/></p> <p>Portal heartbeat verification: <input checked="" type="checkbox"/> <input type="checkbox"/></p> <p>*Portal key: <input type="text"/> <small>.....</small></p> <p>*Confirm the portal key: <input type="text"/> <small>.....</small></p> <p>URL key: <input type="text"/></p> <p>Confirm URL key: <input type="text"/></p> <p>Terminal IP address list: <input type="text"/></p> <p>*Portal authentication port: 2000</p> <p>Service-Type settings: <input checked="" type="checkbox"/></p>
--	---

Portal Authentication Issue (1/3) — Authentication Failure

- Check whether the shared key is configured on the WAC.
 - Error-prone configuration: The shared key configured on the WAC must be the same as that on the server.
 - Suggestion: Reconfigure the shared key and then perform the Portal user authentication test.

```
[WAC] web-auth-server portal  
[WAC-web-auth-server-portal] share-key cipher XXXX (shared key, which must be the same as that configured on the Portal server)  
[WAC-web-auth-server-portal] quit
```
- Check whether STA address learning is disabled on the WAC.
 - Error-prone configuration: When processing an authentication request from the Portal server, the WAC searches for user MAC addresses based on user IP addresses. If the user IP addresses are not reported by APs, the WAC does not record the user IP addresses. As a result, the WAC fails to find the matched user MAC addresses based on the recorded user IP addresses, and thereby cannot process the authentication request.
 - Suggestion: Enable STA address learning.

```
[WAC-wlan-view] vap-profile name portal  
[WAC-wlan-vap-prof-portal] undo learn-client-address ipv4 disable
```

Portal Authentication Issue (2/3) — Portal Server Not Automatically Pushing an Authentication Page

- Check whether the detection function is enabled in the **web-auth-server** profile.
 - Error-prone configuration: The detection function is enabled on the WAC, but the Portal server is not enabled. In this case, the Portal server status is displayed as **Abnormal** on the WAC.

```
[WAC] web-auth-server portal  
[WAC-web-auth-server-portal] server-detect  
[WAC-web-auth-server-portal] quit
```
 - Suggestion: If the Portal server does not support the heartbeat detection function or the heartbeat detection function is not enabled, disable the detection function on the WAC.

```
[WAC] web-auth-server portal  
[WAC-web-auth-server-portal] undo server-detect  
[WAC-web-auth-server-portal] quit
```

Portal Authentication Issue (3/3) — iOS Terminals Not Automatically Displaying an Authentication Page

- Check whether the Portal bypass function is configured on the WAC.
 - Error-prone configuration: The Portal bypass function is enabled on the WAC.
[WAC] portal captive-bypass enable
▫ Suggestion: Disable the Portal bypass function and perform the test again.
[WAC] undo portal captive-bypass enable
- Check whether the Portal server pushes an authentication page through HTTPS.
 - Error-prone configuration: If the Portal server pushes an authentication page through HTTPS, but no valid certificate issued by the CA is installed on the Portal server, the Portal authentication page is not automatically displayed on iOS terminals.
 - Suggestion: Check whether the Portal server pushes an authentication page through HTTPS. If so, you are advised to install a valid certificate or change the protocol to HTTP for authentication page pushing.

MAC Authentication Configuration — WAC

- Configure a security profile (same as the Portal authentication configuration).
- Configure an access profile.

```
[WAC] mac-access-profile name test  
[WAC-mac-access-profile-test] quit
```

- Configure the RADIUS server (same as the 802.1X authentication configuration).
- Configure an AAA scheme (same as the 802.1X authentication configuration).
- Configure an authentication profile.

```
[WAC] authentication-profile name mac  
[WAC-authentication-profile-mac] mac-access-profile mac  
[WAC-authentication-profile-mac] access-domain test  
[WAC-authentication-profile-mac] quit
```

- Apply the authentication profile and security profile.

```
[WAC-wlan-view] vap-profile name mac  
[WAC-wlan-vap-prof-mac] authentication-profile mac  
[WAC-wlan-vap-prof-mac] security-profile test  
[WAC-wlan-vap-prof-mac] quit
```

MAC Authentication Configuration — iMaster NCE-Campus (1/2)

- Add an admission device. Choose **Admission > Admission Resources > Admission Device > Admission Device Management**, click **Create** to add a WAC, as shown in the following figure.

Admission / Admission Resources / Admission Device

Admission Device Management

Admission Regions Admission Device Template

Third-party Admission Device Cloud Managed Admission Device

Device Name	Description	IP Address	Backup IP Address	Device Series	RADIUS Authent...	Portal Authentica...	HWTACACS Aut...	Operation
WAC1		10.23.100.1	--	Huawei NAC	Configured	Configured	Not configured	

Transfer Export Import Delete Create

- Add an authentication user. Choose **Admission > Admission Resources > User Management > User Management > MAC Account**, click **Create** to add a MAC account, as shown in the following figure.

Admission / Admission Resources / User Management

User Management Role Management Blacklist Management

User **MAC Account** PPSK User Operation Log

Filter

MAC Account Name	MAC List	Status	User Group	Role	Email	Contact Number	Expiration Time	Description	Operation
mac-user	08***B4.28***32	Enabled	ROOT/HCIP-WLAN						

Custom Field Disable Enable Export Import Delete Create

MAC Authentication Configuration — iMaster NCE-Campus (2/2)

- Configure authentication and authorization rules, which can be matched by end users based on specific conditions.
 - Choose **Admission > Admission Policy > Authentication and Authorization > Authentication Rules**, modify the default authentication rule or create an authentication rule.

Admission / Admission Policy / Authentication and Authorization

Authentication Rules		Authorization Result	Authorization Rules	Policy Element
Enter a name <input type="text"/> <input type="checkbox"/> Priority <input type="text"/> Name <input type="text"/> Authentication <input type="text"/> Access Mode <input type="text"/> Matching Condition				<input type="button" value="Disable"/> <input type="button" value="Enable"/> <input type="button" value="Delete"/> <input type="button" value="Create"/>
<input type="checkbox"/> 1 <input type="text"/> MAC <input type="text"/> MAC address <input type="text"/> Wireless		<input type="radio"/> User group <input type="text"/> ROOTHCIP-WLAN	<input type="radio"/> SSID <input type="text"/> wlan-net	Data Source <input type="text"/> Authentication <input type="text"/> Access Policy <input type="text"/> Enabling Status <input type="text"/> Operation
				PAP protocol <input type="text"/> <input type="button" value="Enable"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

- Choose **Admission > Admission Policy > Authentication and Authorization > Authorization Rules**, associate the authorization result and specify the resources that can be accessed by authenticated users.

Admission / Admission Policy / Authentication and Authorization

Authentication Rules		Authorization Result	Authorization Rules	Policy Element
Enter a name <input type="text"/> <input type="checkbox"/> Priority <input type="text"/> Name <input type="text"/> Authentication <input type="text"/> Access Mode <input type="text"/> Matching Condition				<input type="button" value="Disable"/> <input type="button" value="Enable"/> <input type="button" value="Delete"/> <input type="button" value="Create"/>
<input type="checkbox"/> 1 <input type="text"/> MAC <input type="text"/> MAC address <input type="text"/> Wireless		<input type="radio"/> User group <input type="text"/> ROOTHCIP-WLAN	<input type="radio"/> SSID <input type="text"/> wlan-net	Authorization <input type="text"/> Description <input type="text"/> Enabling Status <input type="text"/> Operation
				Permit Access <input type="button" value="Enable"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

Quiz

1. (Multiple-Answer Question) After a user is authenticated, which of the following permissions can be delivered by Huawei devices? ()
 - A. VLAN
 - B. IP address
 - C. ACL
 - D. UCL group

1. ACD

Summary

- NAC is the first line of defense to ensure cyber security. To implement NAC, you can deploy user authentication modes including MAC authentication, 802.1X authentication, and Portal authentication on the network. The implementation modes and application scenarios of these technologies are different. Therefore, you need to select and deploy them based on network characteristics and actual requirements.
- Upon completion of this course, you have understood the implementation principles of various access authentication technologies and been able to independently build Huawei's access control networks.

Recommendations

- Huawei official websites:
 - Enterprise service: <https://e.huawei.com/en/>
 - Technical support: <https://support.huawei.com/enterprise/en/index.html>
 - Online learning: <https://www.huawei.com/en/learning>

Acronyms and Abbreviations (1/3)

Acronym/Abbreviation	Full Name
AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
AD	Active Directory
ARP	Address Resolution Protocol
C/S	Client/Server
CHAP	Challenge Handshake Authentication Protocol
CoA	Change of Authorization
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol version 6
DM	Disconnect Message
EAP	Extensible Authentication Protocol

Acronyms and Abbreviations (2/3)

Acronym/Abbreviation	Full Name
EAP-MD5	EAP-Message Digest Algorithm 5
EAPoL	EAP over LAN
EAPoR	EAP over RADIUS
EAP-PEAP	EAP-Protected Extensible Authentication Protocol
EAP-TLS	EAP-Transport Layer Security
EAP-TTLS	EAP-Tunneled Transport Layer Security
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
ND	Neighbor Discovery

Acronyms and Abbreviations (3/3)

Acronym/Abbreviation	Full Name
PAP	Password Authentication Protocol
PPP	Point-to-Point Protocol
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
STA	Station
TCP	Transmission Control Protocol
UCL	User Control List
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VPDN	Virtual Private Dial-up Network
WAC	Wireless Access Controller

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。
Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

Copyright©2022 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product performance, market position, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.



Comprehensive Cases of Enterprise Network Security



Foreword

- The courses of security technologies describe how to deploy and apply each single technology. On real networks that may face diverse security challenges, comprehensive use of these technologies is usually required. As such, security implementation engineers need to comprehensively consider various security threats and countermeasures, assist in designing network security solutions, determine the feasibility of the solutions, and finally implement the solutions. Network security O&M engineers need to pay attention to the network security situation and respond to detected security threats in a timely manner to protect enterprise network security and reduce enterprise property loss.
- This course describes how to use different technologies to design and implement a network security solution based on live network requirements.

Objectives

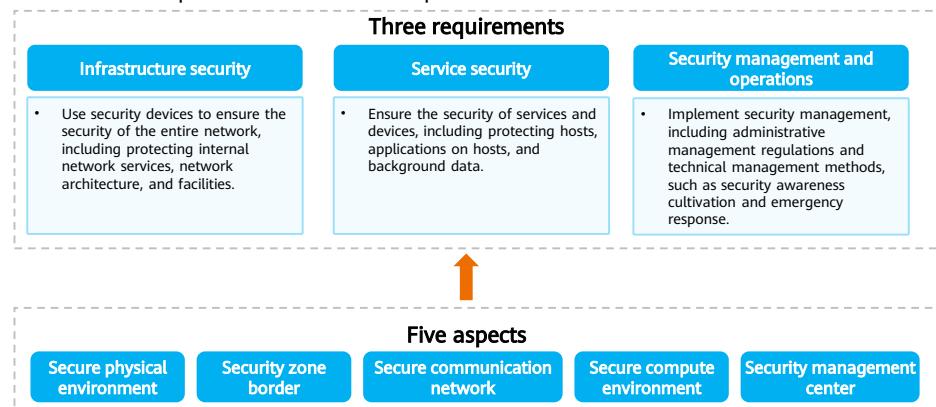
- Upon completion of this course, you will be able to:
 - Apply various network security technologies.
 - Design the network security solution.
 - Deploy the network security solution.
 - Be familiar with network security O&M.

Contents

- 1. Overview of Enterprise Network Security Requirements**
2. Enterprise Network Security Solution Design and Deployment
3. Enterprise Network Security Troubleshooting

Overview of Enterprise Network Security Requirements

- Enterprise network security requirements are classified into three aspects, which are usually fulfilled from five technical aspects based on the enterprise's structure.



4 Huawei Confidential

 HUAWEI

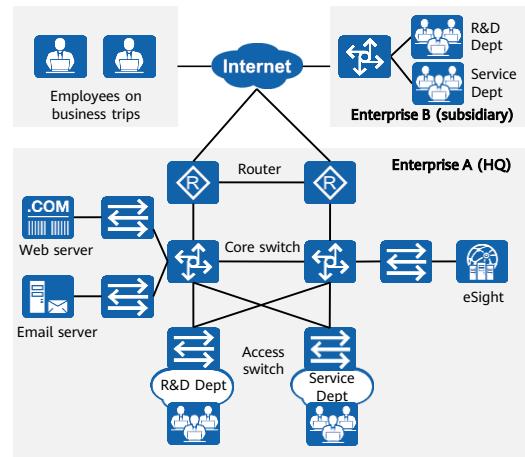
- This course describes how to design and deploy an enterprise network based on the preceding security requirements and solutions.

Contents

1. Overview of Enterprise Network Security Requirements
2. **Enterprise Network Security Solution Design and Deployment**
 - Network Requirements and Solution Overview
 - Communication Network Design
 - Border Zone Design
 - Compute Environment Design
 - Management Center Design
3. Enterprise Network Security Troubleshooting

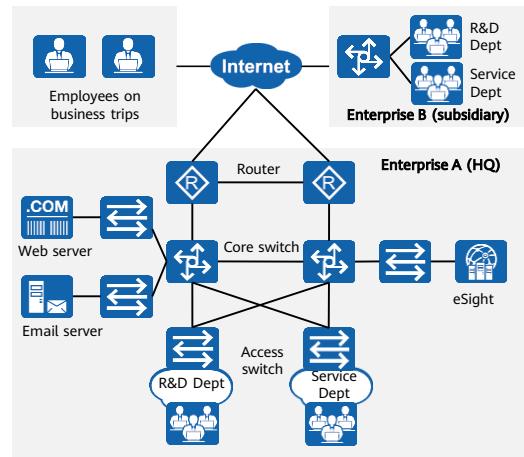
Example of Enterprise Network Security Requirements (1/2)

- The figure on the right shows the current network topology of a game company that owns two enterprises (A is the HQ and B is its subsidiary). Considering that the services of the company may face many security threats, network implementation engineers need to optimize the network topology for security purposes.
 - Security requirement 1: Redundant devices and links need to be deployed on key nodes of enterprise A's network, and high-quality links carry a large amount of traffic.
 - Security requirement 2: The security of communication between enterprise A and enterprise B needs to be ensured.
 - Security requirement 3: Identity authentication needs to be performed for employees on business trips to ensure the security of external access to the internal network.
 - Security requirement 4: To ensure employees' work efficiency, both enterprises need to limit employees' traffic and bandwidth usage during working hours without affecting email and file transfer services.



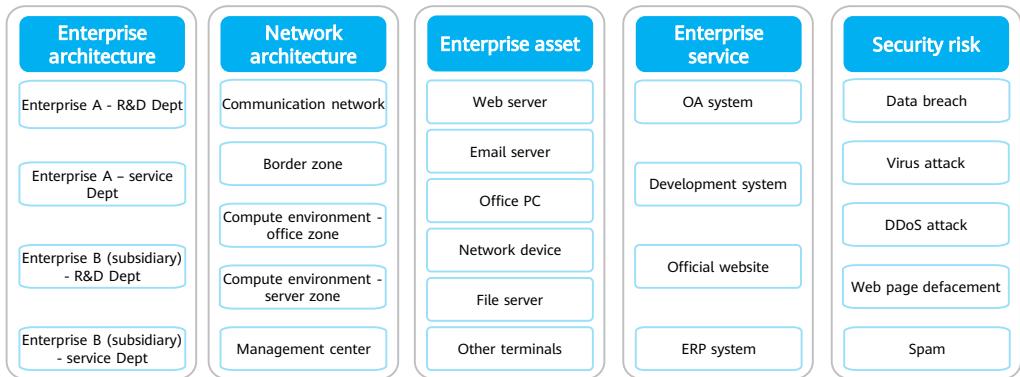
Example of Enterprise Network Security Requirements (2/2)

- Security requirement 5: Enterprise B specializes in product R&D and has external service departments. Therefore, the R&D department must be strictly isolated to ensure data security of core services.
- Security requirement 6: As the gaming industry is an emerging industry, this game company may face threats such as DDoS attacks, hacker intrusions, and virus attacks. Therefore, security approaches must be developed in advance and subsequent O&M work, such as the feasibility and convenience of emergency response, must be considered.
- Security requirement 7: The identity of internal employees needs to be authenticated when they attempt to access the intranet. In addition, user behaviors need to be controlled. For example, the access rights of specific websites need to be restricted to prevent employees from disclosing information or releasing violation information.
- Security requirement 8: Prevent employees from disclosing confidential information through emails, and prevent spam from occupying too many resources or affecting employees' normal email sending and receiving.



Enterprise Network Security Solution Design Roadmap

- Consider the following factors when designing an enterprise network security solution. The preceding case is used as an example.

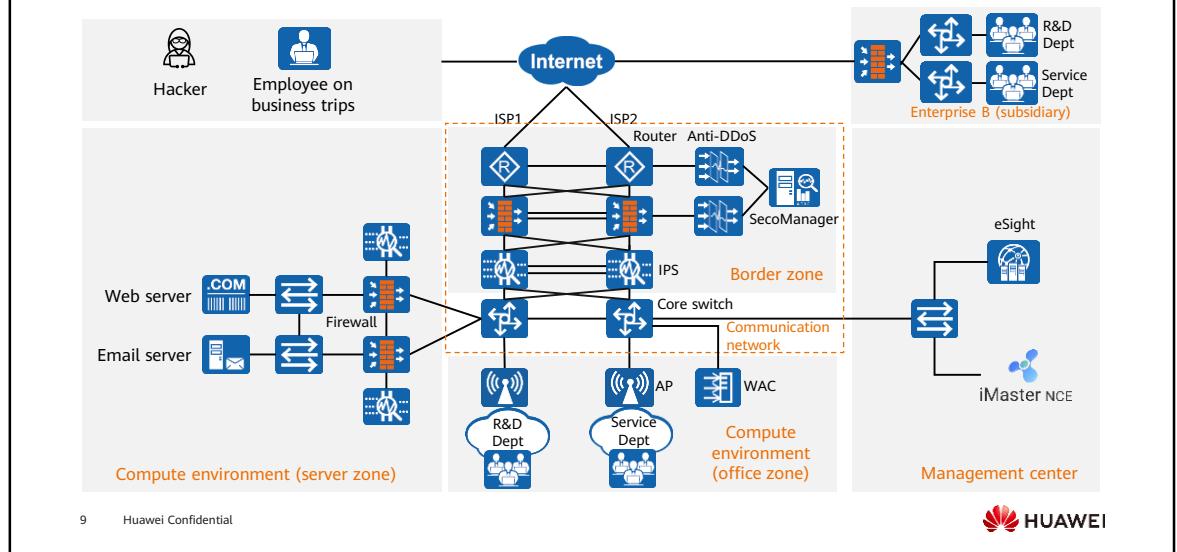


8 Huawei Confidential



- The enterprise architecture, network architecture, enterprise assets, enterprise services, and security risks, as well as the feasibility and convenience of network O&M must be considered for designing enterprise network security.
- The preceding enterprise assets and services are an example.
 - Enterprise architecture: Both the HQ and its subsidiary consist of the R&D and service departments. The HQ has a large number of employees and a large network scale. The subsidiary is in the initial stage. The HQ assigns a game module development task to the subsidiary. The subsidiary has a small number of employees and a small network scale.
 - Network architecture: Based on network security rules, the network architecture is divided into the communication network, border zone, compute environment, and management center.
 - Enterprise assets: include terminals (such as servers and computers) and network devices.
 - Enterprise service: The company has the internal management system, official website, and the unique development system of a game company.
 - Security risks: The company may encounter common threats such as data breach and virus attacks and the DDoS attacks targeting game companies.

Enterprise Network Security Solution Design



- The enterprise architecture is divided from five aspects to facilitate subsequent technical design based on the requirements.

Contents

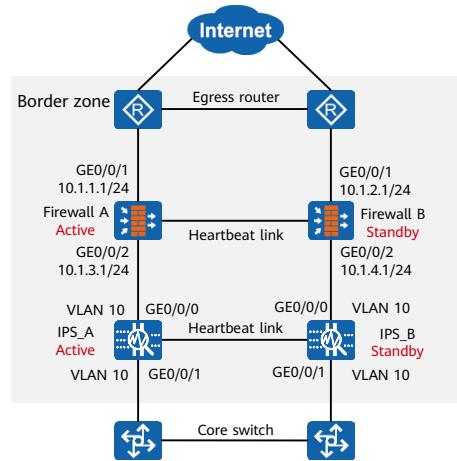
1. Overview of Enterprise Network Security Requirements
2. **Enterprise Network Security Solution Design and Deployment**
 - Network Requirements and Solution Overview
 - **Communication Network Design**
 - Border Zone Design
 - Compute Environment Design
 - Management Center Design
3. Enterprise Network Security Troubleshooting

Device Redundancy

- Design the device redundancy security solution based on security requirement 1: Deploy firewalls and IPS devices in redundancy mode in the egress zone.
 - Firewall: The firewalls are deployed at Layer 3. They are connected to the upstream routers and downstream switches to isolate zones, control traffic, and implement redundancy backup.
 - IPS device: The IPS devices are deployed in dual-device in-path mode. They are connected to the upstream firewalls and downstream Layer 3 switches to implement basic network protection, including antivirus and intrusion prevention.
- Key configurations of firewall hot standby (firewall A is used as an example):
 - Use a dynamic routing protocol to monitor service interfaces on firewalls in hot standby mode.

```
[FW_A] hrp adjust ospf-cost enable  
[FW_A] hrp track interface GE0/0/1  
[FW_A] hrp track interface GE0/0/2
```
- Key configurations of IPS hot standby (IPS_A is used as an example):
 - Service interface monitoring:

```
[IPS_A] hrp track vlan GE0/0/1
```



11 Huawei Confidential

 HUAWEI

- The hot standby principle of the IPS device is the same as that of the firewall.

Link Redundancy

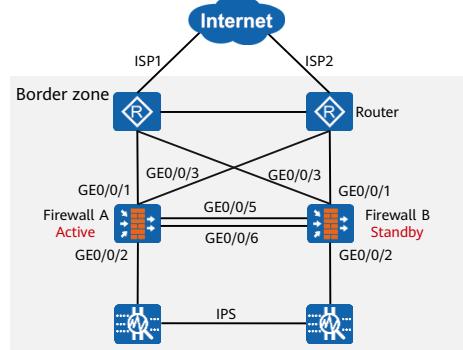
- Design the link redundancy security solution based on security requirement 1: Deploy redundant communication links for devices in the core zone. When links are deployed in redundancy mode, auxiliary technologies need to be deployed. For example, intelligent uplink selection and link aggregation technologies need to be deployed on firewall A.

- Intelligent uplink selection: Traffic is load balanced based on link quality. The health detection result indicates that ISP1 has the lowest packet loss rate, latency, and latency jitter. Key configurations are as follows:

```
[FW_A] multi-interface  
[FW_A-multi-inter] mode priority-of-link-quality  
[FW_A-multi-inter] add interface GigabitEthernet 0/0/1  
[FW_A-multi-inter] add interface GigabitEthernet 0/0/3
```

- Link aggregation: improves the reliability of heartbeat links. Links are manually aggregated. The number of member interfaces is 2, and the minimum number of active links is 2. Key configurations are as follows:

```
[FW_A] Interface Eth-Trunk 1  
[FW_A-Eth-Trunk1] trunkport GigabitEthernet 0/0/5  
[FW_A-Eth-Trunk1] trunkport GigabitEthernet 0/0/6
```



- For IPS devices deployed in Layer 2 in-path mode, link aggregation needs to be deployed to improve heartbeat link reliability.
- For core switches, route deployment and route selection must be considered.

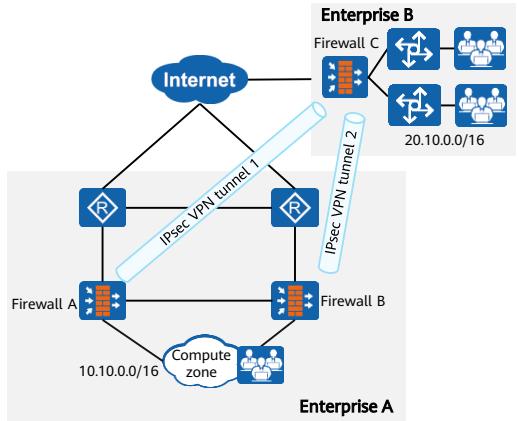
Encrypted Transmission (1/4)

- Design a security solution based on security requirement 2 to ensure communication security between enterprise A and enterprise B: Deploy firewalls at the egress of enterprise B, and deploy an IPsec VPN between the firewalls of enterprise A and enterprise B.
- Key IPsec VPN configurations (firewall A is used as an example):
 - Configure the traffic to be encrypted.

```
[FW_A] acl 3001  
[FW_A-acl-adv-3001] rule permit ip source 10.10.0.0 0.0.255.255 destination 20.10.0.0 0.0.255.255
```
 - Configure NAT traversal.

```
[FW_A] ike peer FW  
[FW_A-ike-peer-FW] nat traversal
```
 - Configure Dead Peer Detection (DPD).

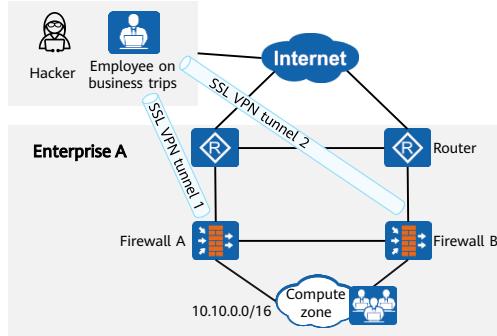
```
[FW_A] ike peer FW  
[FW_A-ike-peer-FW] dpd type on-demand
```



- In enterprise B, IPsec VPN can be deployed on firewalls or routers and switches. Firewalls are deployed to enhance basic security for the network of enterprise B.
- In this example, IP unicast traffic is exchanged between enterprise A and enterprise B, and therefore IPsec VPN is deployed. If non-IP unicast traffic (such as multicast services) is transmitted in actual deployment, GRE over IPsec can be deployed.
- Firewall A and firewall B of enterprise A work in load balancing mode and establish point-to-point IPsec VPN tunnels with firewall C of enterprise B. Tunnels are not backed up. DPD is deployed. When the link from firewall A to firewall C is faulty, traffic forwarded through tunnel 1 is automatically switched to tunnel 2, improving IPsec VPN tunnel reliability.

Encrypted Transmission (2/4)

- Security requirement 3: Identity authentication needs to be performed for employees on business trips to ensure the security of external access to the internal network.
- Security solution: Both L2TP over IPsec and SSL VPN can meet the requirements of employee identity authentication and access confidentiality. Compared with L2TP over IPsec, SSL VPN features simple deployment and configuration and refined permission control. In this solution, SSL VPN is used.



Encrypted Transmission (3/4)

- Key SSL VPN configurations (firewall A is used as an example):

- Virtual gateway

The screenshot shows the 'Modify SSL VPN' configuration page. Under 'Gateway Configuration', the 'Gateway Name' is set to 'security'. The 'Type' is 'Exclusive'. The 'Gateway IP Address' is 'GE0/0/1' with 'IP' '10.1.1.1' and 'Port' '443'. A note at the bottom says 'Note: Enable the security policy to ensure that users log in to the gateway.' There is also a link '[Add Security Policy]'. A red box highlights the 'Gateway IP Address' field.

- Network extension

The screenshot shows the 'Modify SSL VPN' configuration page. Under 'Network Extension', 'Network Extension' is turned on. 'Preserve Connections' is turned on. 'Keepalive Packet Sending Cycle' is set to 120 seconds. 'Available IP Address Range' is '10.10.4.1-10.10.4.254/24'. 'Routing Mode' is set to 'Split routing mode'. A note at the bottom says 'Changing routing mode and internal network segment will make users offline. Please add one network at least in the manual mode or the mode is invalid.' A red box highlights the 'Available IP Address Range' field.

15 Huawei Confidential



Encrypted Transmission (4/4)

▫ Security policy

- Allow Internet users to log in to the virtual gateway.

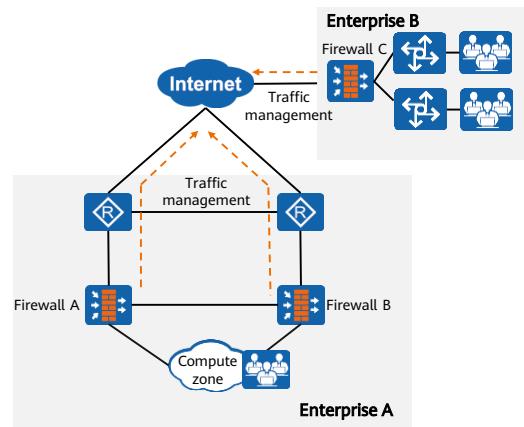
Name	ssl_virtual_gateway
Description	
Policy Group	-- NONE --
Tag	Select or enter a tag.
Source Zone	untrust
Destination Zone	local
Source Address/Region	10.1.1.1 <input type="button" value="X"/>
Destination Address/Region	Select or enter an address.
VLAN ID	Enter a VLAN ID.
User: any; Access Mode: any; Device: any; Service: any; Application: any; URL Category:	
Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny

- Allow network extension users to access intranet resources.

Name	ssl_network
Description	
Policy Group	-- NONE --
Tag	Select or enter a tag.
Source Zone	untrust
Destination Zone	trust
Source Address/Region	10.10.4.0/24 <input type="button" value="X"/>
Destination Address/Region	10.10.2.0/16 <input type="button" value="X"/> 10.10.1.0/16 <input type="button" value="X"/>
VLAN ID	Enter a VLAN ID.
User: any; Access Mode: any; Device: any; Service: any; Application: any; URL Category:	
Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny

Traffic Management (1/2)

- Security requirement 4: To ensure employees' work efficiency, both enterprises need to limit employees' traffic and bandwidth usage during working hours and ensure bandwidth for email and file transfer services.
- Security solution: Configure bandwidth management and quota control policies on the firewalls of enterprises A and B to ensure bandwidth for key services.
 - Bandwidth management: Limits P2P and online video traffic by setting the maximum bandwidth, and guarantees email and file transfer by ensuring the bandwidth.
 - Quota control: The daily Internet access traffic of common employees is limited to 500 MB. When the Internet access traffic exceeds 500 MB, the maximum rate is limited to 200 Kbit/s.



Traffic Management (2/2)

- Key bandwidth management configuration (firewall A is used as an example):

- Configure the guaranteed bandwidth for email and file transfer.

```
[FW_A] traffic-policy  
[FW_A-policy-traffic] profile profile_p2p  
[FW_A-policy-traffic-profile-profile_p2p] bandwidth maximum-bandwidth whole both 30000  
[FW_A-policy-traffic-profile-profile_p2p] bandwidth connection-limit whole both 10000
```

- Configure the maximum bandwidth for P2P and online videos.

```
[FW_A-policy-traffic] profile profile_email  
[FW_A-policy-traffic-profile-profile_email] bandwidth guaranteed-bandwidth whole both 60000
```

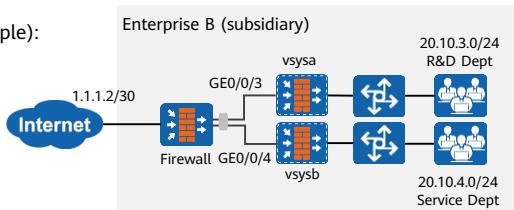
- Key quota control configuration:

- Limit employees' daily Internet access traffic.

```
[FW_A] quota-policy  
[FW_A-policy-quota] profile quota_employee  
[FW_A-policy-quota-profile-quota_employee] stream-daily 500  
[FW_A-policy-quota-profile-quota_employee] limit-bandwidth 200
```

Network Isolation

- Security requirement 5: Enterprise B specializes in product R&D and needs to interconnect with the service department. Therefore, the R&D department must be strictly isolated to ensure the security of core data.
- Security solution: The network architecture of enterprise B is simple and only one firewall is deployed. Deploy virtual systems on the firewall to isolate the service department from the R&D department. Create independent virtual systems **vsysa** and **vsysb** for the R&D department and service department, respectively. The service department can access the Internet, but the R&D department cannot. The service department and R&D department cannot communicate with each other.
- Key virtual system configuration (vsysa is used as an example):
 - Configure a route for vsysa to access the Internet.
`[vsysa] ip route-static 0.0.0.0 0.0.0.0 public`
 - Configure a router for the public system to access the Internet (assume that 1.1.1.2 is the next hop from the public system to the Internet):
`[FW] ip route-static 0.0.0.0 0.0.0.0 1.1.1.2`

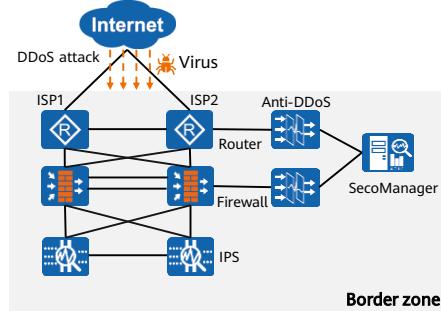


Contents

1. Overview of Enterprise Network Security Requirements
2. **Enterprise Network Security Solution Design and Deployment**
 - Network Requirements and Solution Overview
 - Communication Network Design
 - **Border Zone Design**
 - Compute Environment Design
 - Management Center Design
3. Enterprise Network Security Troubleshooting

Attack Defense (1/3)

- Security requirement 6: Prevent cyber attacks, such as DDoS attacks, hacker intrusions, and virus attacks.
- Security solution: Use anti-DDoS devices to defend against DDoS attacks, and deploy intrusion prevention and antivirus functions on IPS devices.



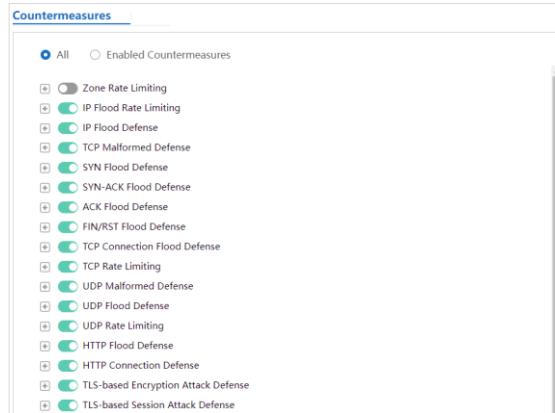
21 Huawei Confidential

 HUAWEI

- IPS intrusion prevention technology: is deployed on IPS devices to protect the compute zone and management center. It detects and defends against intrusions in the upload or download direction of servers or clients, for example, SQL injection by hackers to intranet web servers.
- IPS antivirus technology: is deployed on IPS devices to protect the compute zone and management center. It detects and defends against malicious code attacks, such as viruses, worms, and Trojan horses, when users access the Internet or when Internet access to intranet servers is allowed. For example, intranet users receive infected emails.
- To defend against APT attacks, an enterprise needs to deploy intrusion prevention and antivirus prevention technologies on the IPS device and interwork the IPS device with the sandbox. The sandbox is not described in this course.

Attack Defense (2/3)

- The key anti-DDoS configuration is as follows. The following uses web server protection as an example to describe how to enable defense policies as required.



Attack Defense (3/3)

- Key intrusion prevention configuration on IPS devices:

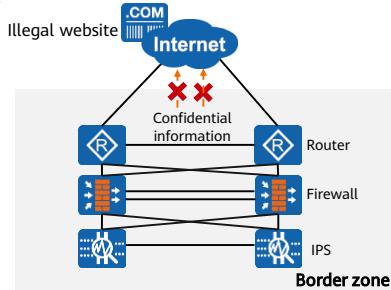
Name	ips_default
Description	
Policy Group	-- NONE --
Tag	Select or enter a tag
Source Zone	any;Destination Zone: any;Source Address/Region: any;Destination Address/Region: any;
Service	any;Application: any;Schedule: any;
Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny
Antivirus	-- NONE --
Intrusion Prevention	<input checked="" type="radio"/> default <input type="radio"/> -- NONE --
Cloud Access Security Awareness	-- NONE --
APT Defense	-- NONE --
URL Filtering	<input type="checkbox"/>

- Key antivirus configuration on IPS devices:

Name	AV_default
Description	
Policy Group	-- NONE --
Tag	Select or enter a tag
Source Zone	any;Destination Zone: any;Source Address/Region: any;Destination Address/Region: any;
Service	any;Application: any;Schedule: any;
Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny
Antivirus	<input checked="" type="radio"/> default <input type="radio"/> -- NONE --
Intrusion Prevention	-- NONE --
Cloud Access Security Awareness	-- NONE --
APT Defense	-- NONE --
URL Filtering	<input type="checkbox"/>

Content Security (1/2)

- Security requirement 7: When employees access the intranet, user behaviors need to be controlled, for example, the access permission of specific websites needs to be restricted.
- Security solution: Deploy the content security filtering technology on the firewall to restrict improper user behaviors.
 - Data filtering: When intranet users upload confidential enterprise information or release violation information, the firewall identifies and blocks the information in a timely manner.
 - URL filtering: The enterprise allows employees to access portal and science websites, but prohibits employees from accessing entertainment and illegal websites.



24 Huawei Confidential

 HUAWEI

- Content security filtering technologies include URL filtering, DNS filtering, file blocking, application behavior control, mail filtering, and data filtering. In this example, data filtering, URL filtering, and mail filtering are deployed. When designing and implementing a security solution on the live network, network engineers need to formulate measures based on the actual requirements and security risks of the enterprise.

Content Security (2/2)

- Key data filtering configuration on the firewall:

The screenshot shows two configuration pages for a firewall. The top part, 'Add Keyword Group', has a 'Name' field set to 'content'. The bottom part, 'Modify Data Filtering Rule', shows a rule with 'Name' 'content', 'Keyword Groups' 'content', 'Application' 'all', 'File Type' 'all', 'Word Boundary' set to 'Both', and 'Action' set to 'Block'. A note at the bottom states: 'Note: NFS cannot be blocked. If a restricted file is transmitted over NFS, the alert action will be executed.'

- Key URL filtering configuration on the firewall:

The screenshot shows two URL filtering configuration pages. The top part, 'URL Filtering Level', has 'Medium' selected. The bottom part, 'Search Engines/Portals', lists 'Portals' and 'Search Engines' under the 'Search Engines/Portals' category. The 'Recreation' section is also shown.

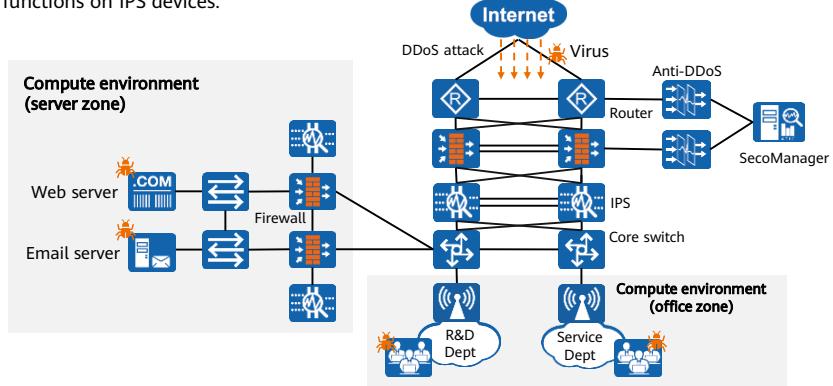
- Note: When configuring a URL filtering policy, you need to configure two URL filtering profiles. In one profile, set the URL filtering level to medium to block all illegal websites and allow access to search/portal and entertainment websites. Apply the profile to a security policy and set the action of the security policy to permit. The other URL filtering profile denies access to entertainment websites. Apply it to a security policy. Set the time range to working hours and the action to permit for the security policy. This security policy needs to be pinned on top.

Contents

1. Overview of Enterprise Network Security Requirements
2. **Enterprise Network Security Solution Design and Deployment**
 - Network Requirements and Solution Overview
 - Communication Network Design
 - Border Zone Design
 - **Compute Environment Design**
 - Management Center Design
3. Enterprise Network Security Troubleshooting

Attack Defense

- Security requirement 6: Prevent cyber attacks, such as DDoS attacks, hacker intrusions, and virus attacks.
- Security solution: Use anti-DDoS devices to defend against DDoS attacks, and deploy intrusion prevention and antivirus functions on IPS devices.



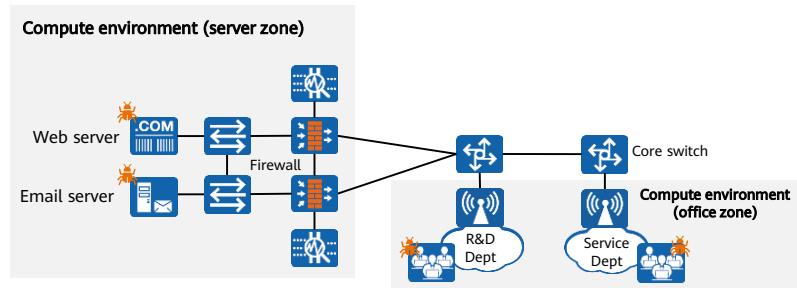
27 Huawei Confidential

HUAWEI

- The key configurations are similar to those on the anti-DDoS and IPS devices in the border zone design and are not described here.

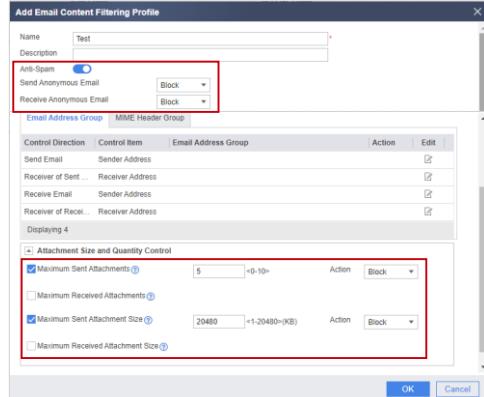
Content Security (1/2)

- Security requirement 7: When employees access the intranet, user behaviors need to be controlled, for example, the access permission of specific websites needs to be restricted.
- Security requirement 8: Prevent employees from disclosing confidential information through emails, and prevent spam from occupying too many resources or affecting normal email sending and receiving.
- Security solution: Deploy the content security filtering technology on the firewall to restrict improper user behaviors.
 - Mail filtering: manages and controls the mail receiving and sending behavior, including preventing flooding of spam and anonymous mails and controlling unauthorized mail receiving and sending.



Content Security (2/2)

- Key mail filtering configuration: On the firewall, limit the size of attachments to be sent to no more than 20 MB and the number of attachments to be sent to no more than 5. Anonymous mails are not allowed to be sent or received, and spam needs to be filtered out.

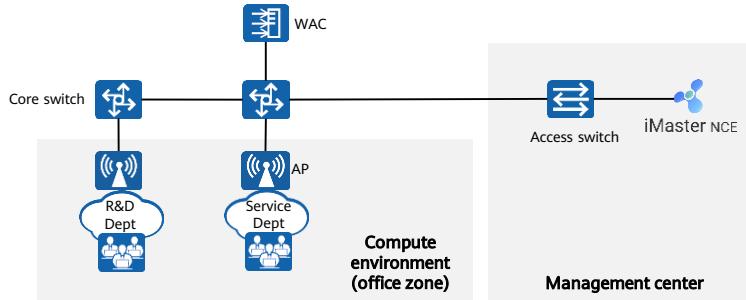


Contents

1. Overview of Enterprise Network Security Requirements
2. **Enterprise Network Security Solution Design and Deployment**
 - Network Requirements and Solution Overview
 - Communication Network Design
 - Border Zone Design
 - Compute Environment Design
 - Management Center Design
3. Enterprise Network Security Troubleshooting

Access Control (1/3)

- Security requirement 7: The identity of an internal employee who attempts to access the intranet needs to be authenticated. The employee can access the network only after passing the authentication. In addition, user behaviors need to be controlled.
- Security solution: Deploy the access control server iMaster NCE-Campus in the management center to authenticate the identity of the internal employees who attempt to access the intranet and assign different access permissions based on the employees' roles. In addition, the access network needs to be provided for guests to restrict their access rights.



Access Control (2/3)

- Key iMaster-NCE campus configuration: Create authentication and authorization rules based on the authentication mode and network access rights.

The image contains two screenshots of the iMaster-NCE interface, both titled "Admission / Admission Policy / Authentication and Authorization".

Screenshot 1: Authentication Rules

This screenshot shows the "Authentication Rules" tab selected. It displays a table with one row of data:

Priority	Name	Authenticatio...	Access Mode	Matching Condition	User group	SSID	Data Sour...	Authentic...	Access P...	Enabling Sta...	Operation
1	802.1X	User access...	Wireless		ROOTHCIP-WLAN	wlan-net	<Data sour...	EAP-PEAP...	-	-	Enable

Screenshot 2: Authorization Rules

This screenshot shows the "Authorization Rules" tab selected. It displays a table with one row of data:

Priority	Name	Authenticatio...	Access Mode	Matching Condition	User group	SSID	Authorizatio...	Description	Enabling Sta...	Operation	
1	802.1X	User access...	Wireless		ROOTHCIP-WLAN	wlan-net	Permit Access		Enable		

Access Control (3/3)

- Key WAC configuration: After authentication configurations are complete, you need to configure corresponding permissions on the device to ensure that authorization permissions can be successfully delivered. The following uses user group-based authorization as an example:

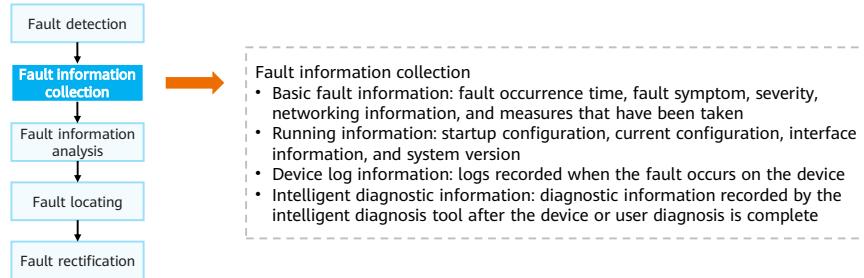
```
[WAC] acl 3001
[WAC-acl-adv-3001] rule 1 permit ip destination 10.23.200.2 0
[WAC-acl-adv-3001] rule 2 deny ip destination any
[WAC-acl-adv-3001] quit
[WAC] user-group group1
[WAC-user-group-group1] acl-id 3001
[WAC-user-group-group1] quit
```

Contents

1. Overview of Enterprise Network Security Requirements
2. Enterprise Network Security Solution Design and Deployment
3. **Enterprise Network Security Troubleshooting**

Troubleshooting Process

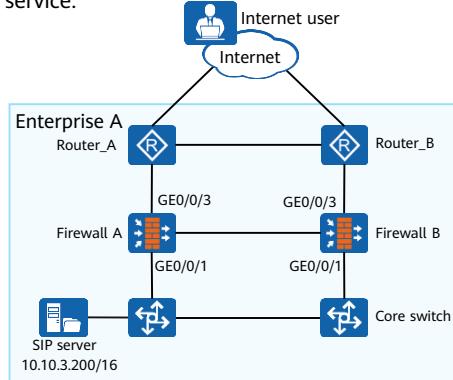
- The basic idea of troubleshooting is to group all possible causes of a fault into multiple cause sets to reduce problem complexity. Troubleshooting is to find fault causes step by step, and finally resolve the fault.
- A fault can be detected on the user side (for example, a user cannot access the Internet) or on the network side (for example, an alarm is generated on a device). After a fault is detected, collect fault information about each device immediately, analyze fault information, and then locate and rectify the fault. For solution-level troubleshooting on the entire network, the key is to quickly locate the fault to a component based on the fault symptom and then rectify the fault.



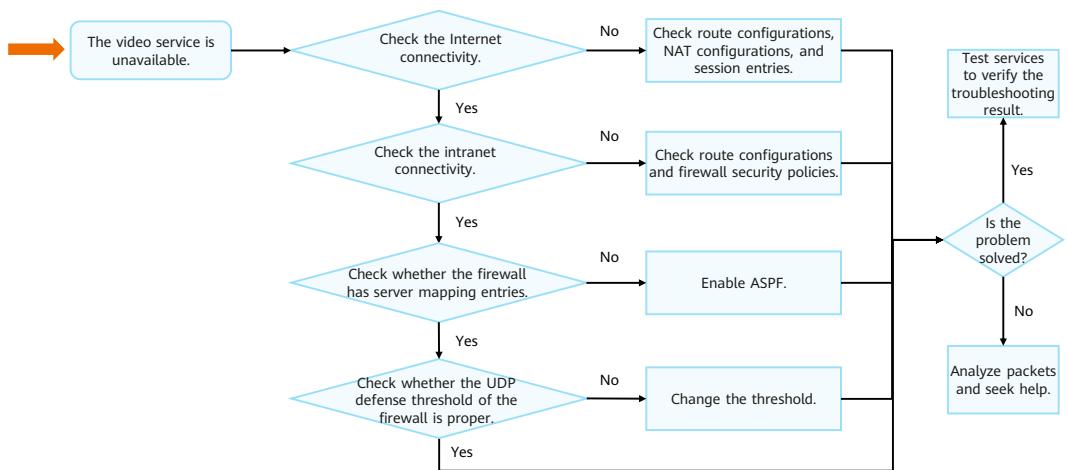
- Troubleshooting principles:
 - Recover the system as soon as possible.
 - During fault locating, collect fault data in a timely manner and save the data to mobile storage media or PCs on the network.
 - Before determining the fault handling solution, evaluate the solution's impact and ensure normal running of services.

Fault 1: Video Service Communication Failure (1/2)

- Symptom: The enterprise needs to add a video conference service for internal conferences or communication with external customers. During service migration verification, it is found that Internet users cannot use the video service.



Fault 1: Video Service Communication Failure (2/2)



Video Service Troubleshooting: Checking Connectivity

- Check the connectivity of the Internet.

- Run the Ping and Tracet commands to check whether the connectivity of the Internet is normal. If an error occurs, check route configurations.
 - Check the NAT policy and mapping. If the configuration is incorrect, modify it.

```
[FW_A] display nat-policy rule all  
[FW_A] display nat server
```

- Check firewall sessions.

```
[FW_A] display firewall session table  
Current Total Sessions : 1  
SIP VPN: public --> public 100.1.1.100:2052 --> 10.10.3.200:5060
```

- If the NAT configuration is incorrect, run the following command to clear the session table for the reconfiguration to take effect immediately:

```
[FW_A] reset firewall session table
```

- Precautions: After you clear the session table, all the connections and services, for which packets are forwarded according to the session table, are forcibly disconnected. A user needs to initiate a connection request again before restarting the communication. So unless necessary, do not clear the session table.
- Checking the internal network connectivity:
 - When testing the internal network connectivity, you can use the ping command or directly access the service. If you use the ping command, you need to allow the ping operation on the firewall for a short period of time. After the test is complete, forbid the ping operation immediately.
 - During security policy troubleshooting, if the security policies of the two firewalls are inconsistent, you need to check the hot standby configuration of the firewalls.

Video Service Troubleshooting: Checking Entries

- Check the server mapping table of the firewall.

```
[FW_A] display firewall server-map
```

- Check whether the ASPF function of the SIP protocol is enabled on the firewall. If not, enable it.

```
[FW_A] firewall detect sip
```

- Check the server mapping table of the firewall again.
- Check the session table of the firewall again.
- Verify the video conference service for Internet users.

Video Service Troubleshooting: Checking UDP Attack Defense Settings on the Firewall

- Check the UDP traffic limiting threshold of the firewall.

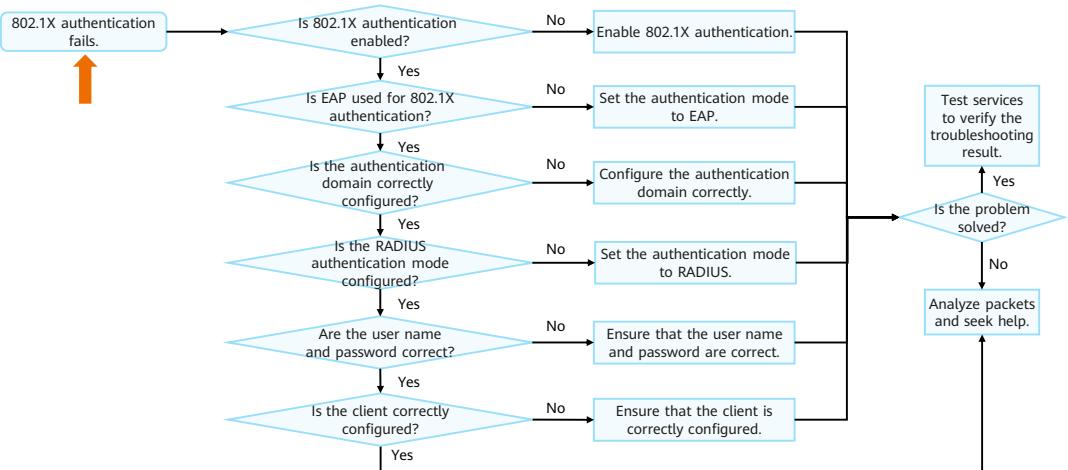
```
[FW_A] display anti-ddos baseline-learn information
```

```
Baseline Learn Information Table -----
```

AttackType	DefendDeployed	AlertRate	LearnResult	Unit
Syn flood attack	Yes	2000	0	pps
UDP flood attack limit	Yes	1	---	Mbps
Icmp flood attack	Yes	2000	0	pps

- It is found that the threshold for UDP traffic limiting is set improperly. As a result, the firewall directly discards the UDP packets that exceed the threshold. The modification solution is as follows:
 - You can adjust the UDP traffic limiting threshold or disable UDP traffic limiting based on service requirements.

Fault 2: Failed to Access the Network — 802.1X



Checking Whether 802.1X Authentication Is Enabled

- Check whether 802.1X access profile **dot1x** is bound to authentication profile **dot1x**.

```
<WAC> system-view  
[WAC] authentication-profile name dot1x  
[WAC-authentication-profile-dot1x] display this  
#  
authentication-profile name dot1x  
dot1x-access-profile dot1x
```

- If not, bind the 802.1X access profile in the authentication profile view.

```
[WAC-authentication-profile-dot1x] dot1x-access-profile dot1x
```

- Check whether authentication profile **dot1x** is bound to VAP profile **dot1x**.

```
[WAC-wlan] vap-profile name dot1x  
[WAC-wlan-vap-prof-dot1x] display this  
#  
forward-mode tunnel  
service-vlan vlan-id 101  
ssid-profile 1  
security-profile 1  
authentication-profile dot1x
```

- If not, bind the authentication profile in the VAP profile view.

```
[WAC-wlan-vap-prof-dot1x] authentication-profile dot1x
```

Checking Whether the User Authentication Mode Is EAP

- 802.1X authentication has three authentication modes: Extensible Authentication Protocol (EAP), Challenge Handshake Authentication Protocol (CHAP), and Password Authentication Protocol (PAP) authentication. Ensure that the authentication client and server use the same authentication mode; otherwise, the client cannot pass 802.1X authentication.
- Mobile terminals such as mobile phones support EAP authentication only. Therefore, EAP authentication also needs to be configured on the device. The default 802.1X authentication mode is EAP.
- Check the authentication mode in the 802.1X access profile **d1**.

```
<WAC> display dot1x-access-profile configuration name dot1x
Profile Name : dot1x
Authentication method : EAP
Re-Authen : Disable
Client-no-response authorize : -
Max retry value : 2
Reauthen Period : 3600s
Client Timeout : 5s
Bound authentication profile : dot1x
```

- To set the authentication method to **EAP**, run the following commands:

```
<WAC> system-view
[WAC] dot1x-access-profile name dot1x
[WAC-dot1x-access-profile-dot1x] dot1x authentication-method eap
```

Checking Whether the Authentication Domain Is Correctly Configured

- When configuring 802.1X authentication, you need to configure AAA schemes, including the authentication scheme profile, authorization scheme profile, accounting scheme profile, and a service scheme profile. If RADIUS authentication is used, you need to configure a RADIUS server template and set parameters for the device to connect to the RADIUS server.
- AAA schemes are directly bound to the authentication profile.

```
[WAC] authentication-profile name dot1x
[WAC-authentication-profile-dot1x] display this
#
authentication-profile name dot1x
dot1x-access-profile dot1x
authentication-scheme radius
accounting-scheme radius
radius-server radius
#
```

- A domain is bound to the authentication profile.

```
[WAC-aaa] domain radius
[WAC-aaa-domain-radius] display this
#
domain radius
authentication-scheme radius
accounting-scheme radius
radius-server radius
#
```

```
[WAC] authentication-profile name dot1x
[WAC-authentication-profile-dot1x] display this
#
authentication-profile name dot1x
dot1x-access-profile dot1x
access-domain radius
#
```

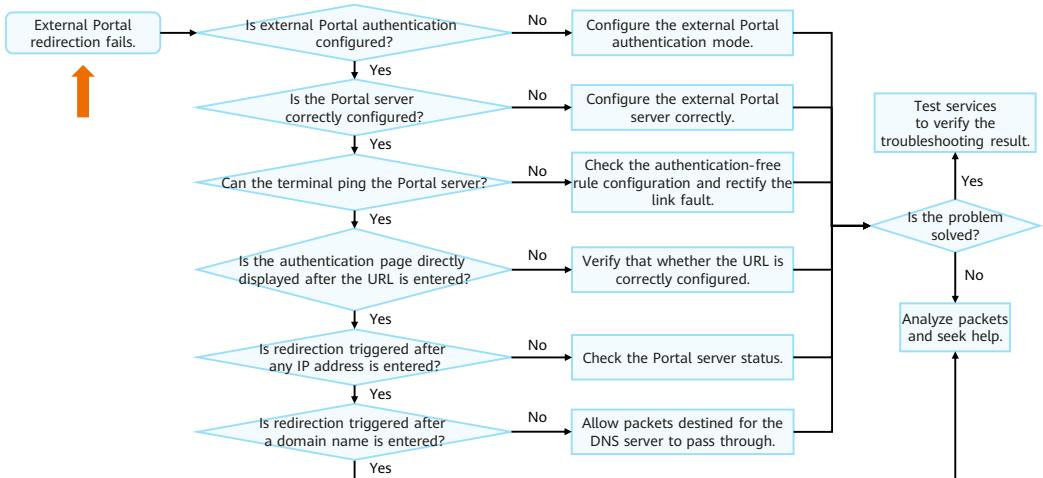
- The preceding configurations can be implemented in either of the following ways:
 - Bind the AAA scheme to an authentication profile.
 - Bind the AAA scheme to the domain and then bind the domain to the authentication profile.
- If both the methods are used, the AAA scheme bound to the authentication profile takes effect preferentially. In this case, check the configuration mode of AAA schemes in the authentication profile and then check whether the AAA scheme configuration is correct in the corresponding view.

Checking the Authentication Mode, User Name, and Password

- If no authentication domain is used, check whether the authentication mode configured in the authentication scheme profile bound to the authentication profile is RADIUS authentication.
- If the authentication domain is used, check whether the authentication mode configured in the authentication scheme profile bound to the authentication domain is RADIUS authentication.
- Run the following commands to check the authentication mode in the authentication scheme profile:
[WAC-aaa] authentication-scheme radius
[WAC-aaa-authen-radius] display this

authentication-scheme radius
 authentication-mode radius
#
- Run the **test-aaa** command to check whether the RADIUS server is reachable and verify the user name and password.
[WAC] test-aaa *test* *huawei123* radius-template *radius*
- In the command output:
 - If the message "Account test succeed" is displayed, the link between the device and RADIUS server is normal, and the user name and password are correct.
 - If the message "User name or password is wrong" is displayed, the link between the device and RADIUS server is normal, but the user name or password is incorrect. You need to check the user name and password.
 - If the message "Account test time out" is displayed, the device and RADIUS server are unreachable or the RADIUS server template is incorrectly configured.

Fault 3: External Portal Redirection Fails



Checking Whether the Portal Authentication Configuration Is Correct

- Check whether the external Portal server function is enabled in the Portal access profile.

```
[WAC] portal-access-profile name portal_access_profile  
[WAC-portal-access-profile-portal_access_profile] display this  
#  
portal-access-profile name portal_access_profile  
web-auth-server portal direct
```

- Check whether the Portal access profile is bound to an authentication profile.

```
[WAC] authentication-profile name portal_authen_profile  
[WAC-authentication-profile-portal_authen_profile] display this  
#  
authentication-profile name portal_authen_profile  
portal-access-profile portal_access_profile  
free-rule-template default_free_rule  
#
```

- Check whether the authentication profile is bound to a VAP profile.

```
[WAC-wlan-view] vap-profile name portal_authen_test  
[WAC-wlan-vap-prof-portal_authen_test] display this  
#  
forward-mode tunnel  
service-vlan vlan-id 200  
ssid-profile portal_authen_test  
authentication-profile portal_authen_profile  
#
```

Checking Whether the Portal Server Is Configured Correctly

- Check the configuration of the external Portal server.

```
[WAC] display web-auth-server configuration
Listening port: 2000
Portal: version 1, version 2
Include reply message : enabled
-----
Web-auth-server Name : portal
IP-address          : 192.168.13.1
Shared-key           : %6A%#xZD=PF^$,"+n#W3@LRoBlx^~Hco42X\p@UJawjh#%%^%
Source-IP           : -
Port / PortFlag     : 50100 / NO
URL                 : http://192.168.13.1:8080/PortalServer
URL Template        : portal
Redirection         : Enable
Sync                : Disable
Sync Seconds        : 0
Sync Max-times      : 0
Detect              : Disable
Detect Seconds      : 60
Detect Max-times    : 3
Detect Critical-num : 0
Detect Action        :
Bound Portal profile : portal_test
-----
1 Web authentication server(s) in total
```

Checking Whether the Terminal Can Ping the Portal Server

- If the IP address of the external Portal server cannot be pinged, check whether the authentication-free rule is applied on the AP.

```
[AP] diagnose  
[AP-diagnose] display portal free-rule  
-----  
Dynamic free rule  
destination ip 10.10.10.10 mask 255.255.255.255 source ip x.x.x.x mask 255.255.255.255 vlan x  
Total 1  
.....
```

- Check whether a route destined for the IP address of the external Portal server is configured on the terminal gateway. If not, configure such a route.
- Check whether a route destined for the IP address of the terminal gateway is configured on the Portal server. If not, configure such a route.

Performing the URL Redirection Test

- Enter the URL of the external Portal server in a browser on the terminal to check whether the Portal authentication page is displayed.
- If the Portal authentication page is not displayed, check whether the URL of the external Portal server is correctly configured on the device.
- If a URL template is bound to the Portal server template, run the **display url-template** command to check whether the URL is correctly configured.

```
[WAC] display url-template name portal
Name          : portal
URL           : http://192.168.13.1:8080/PortalServer
Start mark    : ?
Assignment mark: =
Isolate mark  : &
AC IP         :
AC MAC        :
AP IP         :
AP MAC        :
SSID          :
User MAC      :
Redirect URL  :
User IP address:
Sysname       :
Delimiter     :
Format        :
.....
```

Checking Whether URL Parameters Are Correctly Configured

- When a third-party Portal server is connected, the URL may need to carry specified parameters. The Portal server can obtain information about terminals based on these parameters and then provide different web authentication pages for the terminals.
- The parameters carried in a URL include the WAC system name, WAC IP address, WAC MAC address, AP IP address, AP MAC address, SSID with which the user associates, user IP address, user MAC address, and original URL.
- To enable a URL to carry specified parameters, you can only configure parameters in the URL template.

```
[WAC] url-template name portal  
[WAC-url-template-portal] url-parameter ac-ip acip ap-ip apip user-mac usermac
```

Performing the IP Address-based Redirection Test

- In Portal authentication mode, the Portal authentication page should be displayed after any IP address (rather than an IP address that has been added to the authentication-free rule) is entered in a browser.
 - Enter an IP address (rather than an IP address that has been added to the authentication-free rule) in a browser and check whether the Portal authentication page is displayed.
 - If the Portal authentication page is not displayed when you attempt to visit an HTTPS website, enable HTTPS redirection of Portal authentication.
- [WAC] portal https-redirect enable**
- If the Portal authentication page is not displayed, run the following command on the WAC to check the Portal server status:

```
<WAC> display server-detect state
Web-auth-server      :portal
Total-servers       :1
Live-servers        :1
Critical-num        :0
Status              :Normal
IP-address          :192.168.13.1
Status              :UP
```

- If Portal authentication is triggered when you attempt to access an HTTPS website, the browser displays a security prompt, requiring you to click **Continue** to complete Portal authentication.
- Redirection is not supported if the browser or website runs HSTS.
- If the destination port in HTTPS request packets sent by users is a non-well-known port (443), redirection cannot be performed.
- Check the Portal server status on the WAC.
 - If the Portal server status is **Abnormal**, check whether the Portal server supports the detection function and whether the Portal server detection function is enabled.
 - If the Portal server supports the detection function, enable the Portal server detection function.
 - If the Portal server does not support the detection function, run the following commands on the WAC to disable the Portal server detection function:
 - **[WAC] web-auth-server portal**
 - **[WAC-web-auth-server-portal] undo server-detect**

Checking DNS Configurations

- If the Portal authentication page is displayed after an IP address is entered in a browser but is not displayed after a domain name is entered, check whether the IP address of the DNS server has been added to the authentication-free rule.
- Check whether the IP address of the DNS server is added to the authentication-free rule.

```
[WAC] free-rule-template name portal_free_rule  
[WAC-free-rule-portal_free_rule] display this  
#  
free-rule-template name portal_free_rule  
free-rule 1 destination ip 10.72.55.101 mask 255.255.255.255  
#
```

Quiz

1. (Multiple-answer question) Which of the following aspects can be considered during design to meet enterprise security requirements? ()
 - A. Secure physical environment
 - B. Security zone border
 - C. Secure communication network
 - D. Secure compute environment
 - E. Security management center

1. ABCDE

Summary

- This course uses cases to describe the solution design and technical deployment of enterprise network security, as well as the troubleshooting roadmap and key steps.
- Upon completion of this course, you will be able to design security solutions, deploy security technologies, and troubleshoot faults based on actual network requirements. In addition, you will have a more intuitive understanding of the responsibilities and works of network implementation engineers and network security O&M engineers.

Recommendations

- Huawei official websites:
 - Enterprise service: <https://e.huawei.com/en/>
 - Technical support: <https://support.huawei.com/enterprise/en/index.html>
 - Online learning: <https://www.huawei.com/en/learning>

Acronyms and Abbreviations (1/2)

Acronym/Abbreviation	Full Name
AP	Access Point
ASPF	Application Specific Packet Filter
CHAP	Challenge Handshake Authentication Protocol
DDoS	Distributed Denial of Service
DNS	Domain Name Server
DPD	Dead Peer Detection
EAP	Extensible Authentication Protocol
ERP	Enterprise Resource Planning
IPS	Intrusion Prevention System
ISP	Internet Service Provider

Acronyms and Abbreviations (2/2)

Acronym/Abbreviation	Full Name
NAT	Network Address Translation
OA	Office Automation
P2P	Point-to-Point
PAP	Password Authentication Protocol
SIP	Session Initiation Protocol
SSID	Service Set Identifier
URL	Uniform Resource Locator
WAC	Wireless Access Controller

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。
Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

Copyright©2022 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product performance, market position, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.

